

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 02 May 2001 (02.05.01)	
International application No. PCT/JP00/05832	Applicant's or agent's file reference 900392
International filing date (day/month/year) 29 August 2000 (29.08.00)	Priority date (day/month/year) 30 August 1999 (30.08.99)
Applicant HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
 26 March 2001 (26.03.01)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Kiwa Mpay
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

To:

FUKAMI, Hisao
Mitsui Sumitomo Bank
Minamimorimachi Bldg.
1-29, Minamimorimachi 2-chome,
Kita-ku
Osaka-shi, Osaka 530-0054
JAPON

Date of mailing (day/month/year) 17 July 2001 (17.07.01)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 900392	
International application No. PCT/JP00/05832	International filing date (day/month/year) 29 August 2000 (29.08.00)

1. The following indications appeared on record concerning:	
<input type="checkbox"/> the applicant	<input type="checkbox"/> the inventor <input checked="" type="checkbox"/> the agent <input type="checkbox"/> the common representative
Name and Address 1) FUKAMI, Hisao 2) MORITA, Toshio 3) HORII, Yutaka Sumitomo Bank Minamimori-machi Building 1-29, Minamimori-machi 2-chome Kita-ku, Osaka-shi Osaka 530-0054 Japan	State of Nationality
	State of Residence
	Telephone No. 06-6361-2021
	Facsimile No. 06-6361-1731
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:	
<input type="checkbox"/> the person <input type="checkbox"/> the name <input checked="" type="checkbox"/> the address <input type="checkbox"/> the nationality <input type="checkbox"/> the residence	
Name and Address 1) FUKAMI, Hisao 2) MORITA, Toshio 3) HORII, Yutaka Mitsui Sumitomo Bank Minamimorimachi Bldg. 1-29, Minamimorimachi 2-chome, Kita-ku, Osaka-shi, Osaka 530-0054 Japan	State of Nationality
	State of Residence
	Telephone No. 06-6361-2021
	Facsimile No. 06-6361-1731
3. Further observations, if necessary:	
4. A copy of this notification has been sent to:	
<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned
<input checked="" type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Shinji IGARASHI
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

特許協力条約に基づく国際出願願書

SK01PCT87

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、 右記によって作成された。	PCT-EASY Version 2.91 (updated 01.01.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	SK01PCT87
I	発明の名称	情報処理装置及び処理方法
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号
II-5en	Address:	7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	浅野 智之
III-1-4en	Name (LAST, First)	ASANO, Tomoyuki
III-1-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号
III-1-5en	Address:	ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP



特許協力条約に基づく国際出願願書

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

III-2	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor)
III-2-1	この欄に記載した者は	米国のみ (US only)
III-2-2	右の指定国についての出願人である。	
III-2-4ja	氏名(姓名)	大澤 義知
III-2-4en	Name (LAST, First)	OSAWA, Yoshitomo
III-2-5ja	あて名:	141-0001 日本国
		東京都 品川区
		北品川 6丁目7番35号
		ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION
		7-35, Kitashinagawa 6-chome,
		Shinagawa-ku, Tokyo 141-0001
		Japan
III-2-6	国籍(国名)	日本国 JP
III-2-7	住所(国名)	日本国 JP
III-3	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor)
III-3-1	この欄に記載した者は	米国のみ (US only)
III-3-2	右の指定国についての出願人である。	
III-3-4ja	氏名(姓名)	石黒 隆二
III-3-4en	Name (LAST, First)	ISHIGURO, Ryuji
III-3-5ja	あて名:	141-0001 日本国
		東京都 品川区
		北品川 6丁目7番35号
		ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION
		7-35, Kitashinagawa 6-chome,
		Shinagawa-ku, Tokyo 141-0001
		Japan
III-3-6	国籍(国名)	日本国 JP
III-3-7	住所(国名)	日本国 JP
III-4	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor)
III-4-1	この欄に記載した者は	米国のみ (US only)
III-4-2	右の指定国についての出願人である。	
III-4-4ja	氏名(姓名)	光澤 敦
III-4-4en	Name (LAST, First)	MITSUZAWA, Atsushi
III-4-5ja	あて名:	141-0001 日本国
		東京都 品川区
		北品川 6丁目7番35号
		ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION
		7-35, Kitashinagawa 6-chome,
		Shinagawa-ku, Tokyo 141-0001
		Japan
III-4-6	国籍(国名)	日本国 JP
III-4-7	住所(国名)	日本国 JP

特許協力条約に基づく国際出願願書

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

III-5 III-5-1 III-5-2 III-5-4ja III-5-4en III-5-5ja III-5-5en III-5-6 III-5-7	その他の出願人又は発明者 この欄に記載した者は 右の指定国についての出願人である。 氏名(姓名) Name (LAST, First) あて名: Address: 国籍(国名) 住所(国名)	出願人及び発明者である (applicant and inventor) 米国のみ (US only) 大石 丈於 OISHI, Tateo 141-0001 日本国 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国 JP
IV-1 IV-1-1ja IV-1-1en IV-1-2ja IV-1-2en IV-1-3 IV-1-4	代理人又は共通の代表者、通知 のあて名 下記の者は国際機関において右 記のごとく出願人のために行動 する。 氏名(姓名) Name (LAST, First) あて名: Address: 電話番号 ファクシミリ番号	代理人 (agent) 小池 晃 KOIKE, Akira 105-0001 日本国 東京都 港区 虎ノ門二丁目6番4号 第11森ビル No.11 Mori Bldg., 6-4, Toranomon 2-chome, Minato-ku, Tokyo 105-0001 Japan 03-3508-8266 03-3508-0439
IV-2 IV-2-1ja IV-2-1en	その他の代理人 氏名 Name(s)	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent) 田村 榮一; 伊賀 誠司 TAMURA, Eiichi; IGA, Seiji
V V-1	国の指定 広域特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国である 他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国で ある他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR 及びヨーロッパ特許条約と特許協力条約の締約国で ある他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締約国 である他の国
V-2	国内特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

特許協力条約に基づく国際出願願書

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

V-3	国内特許(この版の EASY の配布後に特許協力条約の締約国になった国)	CO コロンビア EC エクアドル	
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。		
V-6	指定の確認から除かれる国	なし (NONE)	
VI-1	先の国内出願に基づく優先権主張		
VI-1-1	先の出願日	2000年06月21日 (21.06.2000)	
VI-1-2	先の出願番号	特願2000-186172	
VI-1-3	国名	日本国 JP	
VI-2	先の国内出願に基づく優先権主張		
VI-2-1	先の出願日	2000年06月21日 (21.06.2000)	
VI-2-2	先の出願番号	特願2000-186173	
VI-2-3	国名	日本国 JP	
VI-3	先の国内出願に基づく優先権主張		
VI-3-1	先の出願日	2000年08月10日 (10.08.2000)	
VI-3-2	先の出願番号	特願2000-243204	
VI-3-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	5	-
VIII-2	明細書	52	-
VIII-3	請求の範囲	9	-
VIII-4	要約	1	absk01pct87.txt
VIII-5	図面	29	-
VIII-7	合計	96	
VIII-8	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-10	包括委任状の写し	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1, VI-2, VI-3	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-18	要約書とともに提示する図の番号	12	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	小池 晃	

特許協力条約に基づく国際出願願書

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

IX-2	提出者の記名押印	
IX-2-1	氏名(姓名)	田村 榮一
IX-3	提出者の記名押印	
IX-3-1	氏名(姓名)	伊賀 誠司

受理官庁記入欄

10-1	国際出願として提出された書類 の実際の受理の日	
10-2	図面 :	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類 を補完する書類又は図面であつ てその後期間内に提出されたも のの実際の受理の日(訂正日)	
10-4	特許協力条約第11条(2)に基づ く必要な補完の期間内の受理の 日	
10-5	出願人により特定された国際調 査機関	ISA/JP
10-6	調査手数料未払いにつき、国際 調査機関に調査用写しを送付し ていない	

国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

PCT手数料計算用紙(願書付属書)

SK01PCT87

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

[この用紙は、国際出願の一部を構成せず、国際出願の用紙の枚数に算入しない]

0	受理官庁記入欄		
0-1	国際出願番号.		
0-2	受理官庁の日付印		
0-4	様式-PCT/R0/101 (付属書)		
0-4-1	このPCT手数料計算用紙は、 右記によって作成された。		PCT-EASY Version 2.91 (updated 01.01.2001)
0-9	出願人又は代理人の書類記号		SK01PCT87
2	出願人		ソニー株式会社
12	所定の手数料の計算		金額/係数 小計 (JPY)
12-1	送付手数料	T	⇒ 18,000
12-2	調査手数料	S	⇒ 72,000
12-3	国際手数料 基本手数料 (最初の30枚まで)	b1	46,200
12-4	30枚を超える用紙の枚数		66
12-5	用紙1枚の手数料 (X)		1,100
12-6	合計の手数料	b2	72,600
12-7	b1 + b2 =	B	118,800
12-8	指定手数料 国際出願に含まれる指定国 数		88
12-9	Number of designation fees payable (maximum 6)		6
12-10	1指定当たりの手数料 (X)		10,000
12-11	合計の指定手数料	D	60,000
12-12	PCT-EASYによる料金の 減額	R	-14,000
12-13	国際手数料の合計 (B+D-R)	I	⇒ 164,800
12-17	納付するべき手数料の合計 (T+S+I+P)		⇒ 254,800
12-19	支払方法	送付手数料: 特許印紙 調査手数料: 特許印紙 国際手数料: 銀行口座への振込み 優先権証明書請求手数料: 特許印紙	

EASYによるチェック結果と出願人による言及

13-1-1	出願人による言及 注釈	6 7 7 3 弁理士 小池 晃 8 6 3 3 弁理士 田村 榮一 9 6 6 7 弁理士 伊賀 誠司
13-2-2	EASYによるチェック結果 指定国	Green? より多くの指定が可能です。(以下の国が指定からは ずされています: JP) 確認してください。 Yellow! "追加する指定国"の欄を用いた指定がなされています が、この欄を用いることなく、更新された最新のメイ ンテナンステーブルを入手し使用することを推奨しま す。

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年12月27日 (27.12.2001)

PCT

(10) 国際公開番号
WO 01/99333 A1(51) 国際特許分類:
G11B 20/10, G10K 15/02, G06F 12/14

H04L 9/00,

(21) 国際出願番号: PCT/JP01/05327

(22) 国際出願日: 2001年6月21日 (21.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-186172 2000年6月21日 (21.06.2000) JP
特願2000-186173 2000年6月21日 (21.06.2000) JP
特願2000-243204 2000年8月10日 (10.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 浅野智之

(ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]. 大石文於 (OISHI, Tateo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

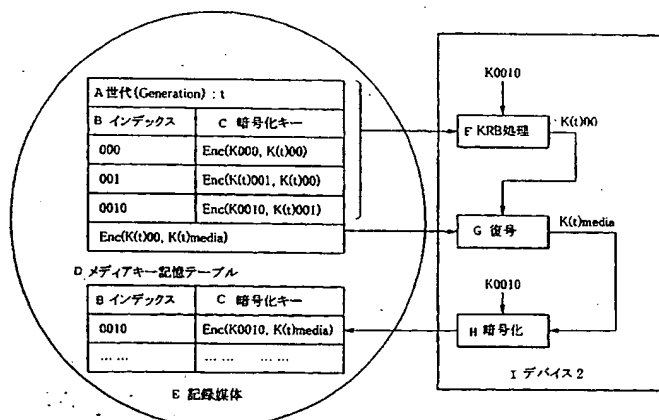
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND PROCESSING METHOD

(54) 発明の名称: 情報処理装置及び処理方法



A...GENERATION (Generation): t F...KRB PROCESSING
B...INDEX G...DECODING
C...ENCRYPTING KEY H...ENCRYPTING
D...MEDIA KEY STORING TABLE I...DEVICE 2
E...RECORDING MEDIUM

(57) Abstract: An information recording/reproducing device for executing a key distribution by a KRB distribution involving a tree-structure key distribution configuration. The device transmits, by using a key-structure key distribution configuration, a key such as a master key, a media key or a content key along with a key update block (KRB). The recording/reproducing device, after calculating and acquiring the key of a certain recording medium based on a reception KRB, encrypts the acquired key using an encryption key specific to the device, for example, a leaf key, and stores it in a recording medium or memory of the device. Therefore, the recording/reproducing device can calculate a key by merely decoding the encrypting key one time when next using the recording medium or contents, and can reduce computational complexity such as KRB decoding required when the device accesses a recording medium or uses contents, thereby making efficient processing on the KRB receiving side.

[続葉有]

WO 01/99333 A1



(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書

(57) 要約:

ツリー（木）構造の鍵配布構成としてのK R B配信によりキーの配布を実行する情報記録再生装置である。この装置は、ツリー構造の鍵配布構成により、マスターキー、メディアキー若しくはコンテンツキー等の鍵をキー更新ブロック（K R B）とともに送信する。記録再生装置が受信K R Bに基づき、ある記録媒体の鍵を計算して取得した後に、取得した鍵を、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する構成とした。従って、記録再生装置が、次にその記録媒体若しくはコンテンツを使用する際に、その暗号化キーを1回復号するだけで鍵を計算でき、記録再生装置が記録媒体にアクセス若しくはコンテンツを利用する際に必要となるK R B復号処理等の計算量を減少させることが可能となり、K R B受信側での処理が効率化される。

明細書

情報処理装置及び処理方法

技術分野

本発明は、情報処理装置及び処理方法、情報記録媒体、並びにコンピュータ・プログラムに関し、特に、ツリー（木）構造の階層的鍵配信方式を用いてコンテンツデータの記録若しくは再生に必要な鍵、例えば、マスターキー、メディアキー若しくはコンテンツキー等を配信若しくは取得し、これを用いて各装置がコンテンツデータの記録若しくは再生を行う構成とした情報処理装置及び処理方法、情報記録媒体、並びにコンピュータ・プログラムに関する。

背景技術

デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、

再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー (copy free) のデータであるか、1度だけコピーが許されている (copy once allowed) データであるか、又はコピーが禁止されている (copy prohibited) データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー (copy free) となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可 (copy once allowed) となっている場合には、SCMS信号をコピー禁止 (copy prohibited) に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、DVD-ROM (Read Only Memory) に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー (復号鍵) が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画

像や音声を再生することができる。

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、正当なライセンスを受けている装置のみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）とにより暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな

記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

上記問題を解決する構成として、本出願人は、各情報記録再生装置を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な鍵（マスターキー若しくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキー若しくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願2000-105328）している。具体的には、記録媒体への記録若しくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えば n 分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、

更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含むキー更新ブロック (K R B: Key Renewal Block) を各情報記録再生装置に配信し、キー更新ブロック (K R B) を受信した各情報記録再生装置の K R B 復号処理により、各装置が記録若しくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

上述のような情報記録再生装置を n 分木の各葉 (リーフ) に配置した構成の鍵配信方法を用いた場合、例えば記録媒体ごとに割り当てられるメディアキーをキー更新ブロック (K R B) で暗号化して配信した場合、各情報記録再生装置は、各記録媒体にアクセスするたびに、すなわち、記録媒体が記録再生装置に装着されるたびに、キー更新ブロック (K R B) 及びデバイスキーを用いたメディアキーの計算を行わなければならない。この計算は、個々の暗号文の復号に要する時間と、メディアキーを暗号化するノードキーから記録再生装置が存在する葉までの木の深さの積に比例するため、装置数が多い、大きな記録システムにおいてはこの処理のオーバーヘッドが大きくなるという問題がある。

また、本出願人は、各情報記録再生装置を n 分木の各葉 (リーフ) に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な暗号鍵としてのコンテンツキーを提供する構成を先に提案し、すでに特許出願 (特願 2 0 0 0 - 1 0 5 3 2 9) している。これは、例えば通信回線を介して、コンテンツデータと、コンテンツデータを暗号化しているコンテンツキーを併せて送付するものであり、コンテンツキーは暗号化データとして送付する構成である。

暗号化コンテンツキーの提供は、例えば n 分木の各葉 (リーフ) を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理したキー更新ブロック (K R B) を用いて行われ、更新ノードキーでコンテンツキーを暗号化して提供することにより、正当な記録再生装置のみがコンテンツキーを取得可能としている。

上述のような情報記録再生装置を n 分木の各葉 (リーフ) に配置した構成の鍵配信方法を用いて暗号化コンテンツキーを提供する場合、各情報記録再生装置は、

コンテンツを利用するたびに、例えば、記録媒体からコンテンツを再生するたびに、KRBをデバイスキー（リーフキー）を用いて処理し、コンテンツキーの計算を行わなければならない。

この計算は、個々の暗号文の復号に要する時間と、コンテンツキーを暗号化するノードキーからデータ処理装置が存在する葉までの木の深さの積に比例するため、装置数が多い、大きなシステムにおいてはこの処理のオーバーヘッドが大きくなるという問題がある。

発明の開示

本発明は、上述の問題を解決するものであり、情報記録再生装置を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用いた構成において、キー更新ブロック（KRB）に基づく暗号化キー又は復号キーの算出処理を省略し、短時間で必要な暗号化キー又は復号キーを取得可能とした構成を提供することを目的とする。具体的には、例えばある記録再生装置がある記録媒体のメディアキーを計算により取得した後に、その取得したメディアキーを、その記録再生装置に固有の暗号鍵を用いて暗号化して格納しておき、次にその記録媒体を使用する際に、その暗号文を1回復号するだけでメディアキーを計算できる構成として、短時間で必要な暗号化キー又は復号キーを取得可能とした情報処理装置、情報処理方法、及び情報記録媒体、並びにコンピュータ・プログラムを提供することを目的とする。

また、本発明は、情報記録再生装置を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用いたコンテンツキーの提供構成において、キー更新ブロック（KRB）に基づく暗号化キー又は復号キーの算出処理を省略し、短時間で必要な暗号化キー又は復号キーとしてのコンテンツキーを取得可能とした構成を提供することを目的とする。具体的には、例えばある記録再生装置がある記録媒体に格納されたコンテンツのコンテンツキーを計算により取得した後に、その取得したコンテンツキーを、その記録再生装置に固有の暗号鍵を用いて暗号化して格納しておき、次にそのコンテンツを再生する際に、その暗号文を1回復号するだけ

でコンテンツキーを計算できる構成として、短時間で必要な暗号化キー又は復号キーとしてのコンテンツキーを取得可能とした情報処理装置、情報処理方法、及び情報記録媒体、並びにコンピュータ・プログラムを提供することを目的とする。

本発明は、暗号化されたデータを処理する情報処理装置であり、この装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理装置内の記憶領域に格納する。

また、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納する。

さらに、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した

復号用キーを、復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて情報処理装置内の記憶領域に格納する。

さらにまた、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、復号処理を実行する復号処理手段を有し、復号処理手段は、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、復号用キーが検出された場合には、記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、復号用キーが検出されなかった場合には、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する。

本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行し、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、この算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納する。

また、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行し、暗号化されたデータを復号処理する際に用い

られる復号用キーの算出処理を実行し、この算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納する。

さらに、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、この算出した復号用キーを、復号用キーを用いて復号されるデータを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納する。

さらにまた、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、復号用キーが検出された場合には、記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、復号用キーが検出されなかった場合には、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する。

本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用い

られる復号用キーの算出処理を実行するステップと、算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行うステップと、暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納するステップとを具備する。

また、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納するステップとを具備する。

さらに、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、算出した復号用キーを、復号用キーを用いて復号されるデータを識別するための識別情報と対応付けて情報処理装置内の記憶領域に格納するステップとを具備する。

さらにまた、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込むステップと、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索するステップと、復号用キーが検出された場合には、記録媒体又は情報処理装置内の記憶領域

に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出するステップと、復号用キーが検出されなかった場合には、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップとを具備する。

そして、本発明は、記録された情報が情報処理装置によって読み出し可能なように構成された情報記録媒体であり、情報処理装置に固有のキーによって暗号化処理を施した、暗号化されたデータを復号するための復号用キーが、情報処理装置の識別情報と関連付けてキー格納テーブルとして記録されている。

本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な鍵（マスターキー、メディアキー若しくはコンテンツキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。ツリー構造の鍵配布構成により、例えばメディアキーの更新をキー更新ブロック（KRB）とともに送信し、記録再生装置が受信KRBに基づき、ある記録媒体のメディアキーを計算して取得した後に、取得したメディアキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する。従って、記録再生装置が、次にその記録媒体を使用する際に、その暗号化キーを1回復号するだけでメディアキーを計算でき、記録再生装置が記録媒体にアクセスする際に必要となるKRB復号処理等の計算量を減少させることが可能となる。

同様に、例えばツリー構造の鍵配布構成により、コンテンツ暗号処理用のコンテンツキーをキー更新ブロック（KRB）とともに送信し、記録再生装置が受信KRBに基づきコンテンツキーを取得した後に、取得コンテンツキーをその記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する。従って、記録再生装置が、次にそのコンテ

ンツを再生利用する際に、その暗号化コンテンツキーを1回復号するだけでコンテンツキーを計算でき、記録再生装置がコンテンツ利用毎にKRB復号処理を実行する必要を排除できる。

なお、本発明のプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。

図面の簡単な説明

図1は、本発明の情報記録再生装置の構成例を示すブロック図である。

図2A及び図2Bは、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図3A及び図3Bは、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図4は、本発明の情報記録再生装置に対するメディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図5A及び図5Bは、本発明の情報記録再生装置に対するメディアキー等の鍵の配布に使用されるキー更新ブロック(KRB)の例を示す図である。

図6は、情報記録再生装置におけるメディアキーのキー更新ブロック(KR

B) を使用した配布例と復号処理例を示す図である。

図 7 は、本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

図 8 は、本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

図 9 は、本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

図 10 は、本発明の情報記録再生装置において適用可能なブロックキーの生成方法を説明する図である。

図 11 は、本発明の情報記録再生装置におけるメディアキーを使用したデータ再生処理時の復号処理を説明するブロック図である。

図 12 は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理例を示す図である。

図 13 は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理フロー (例 1) を示す図である。

図 14 は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理フロー (例 2) を示す図である。

図 15 は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理例を示す図である。

図 16 は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理フローを示す図である。

図 17 は、本発明の情報記録再生装置の変形例におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理、キー格納処理例を示す図である。

図 18 は、本発明の情報記録再生装置に対するコンテンツキー等の鍵の暗号化処理について説明するツリー構成図である。

図 19 A 及び図 19 B は、本発明の情報記録再生装置に対するコンテンツキー

等の鍵の配布に使用されるキー更新ブロック (K R B) の例を示す図である。

図 2 0 は、本発明の情報記録再生装置に対するコンテンツ及びコンテンツキーの提供時のデータ構成例を示す図である。

図 2 1 は、情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用した配布例と復号処理例を示す図である。

図 2 2 は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用した配布例と復号処理、キー格納処理例を示す図である。

図 2 3 は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用したコンテンツ復号処理、キー格納処理フロー (例 1) を示す図である。

図 2 4 は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用したコンテンツ記録処理とキー格納処理フローを示す図である。

図 2 5 は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用したコンテンツ復号処理、キー格納処理例を示す図である。

図 2 6 は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック (K R B) を使用した配布例と復号処理、キー格納処理フローを示す図である。

図 2 7 A 及び図 2 7 B は、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図 2 8 A 及び図 2 8 B は、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図 2 9 は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

以下、本発明の具体的な構成を図面を参照して説明する。

図 1 は、本発明を適用した記録再生装置 1 0 0 の一実施例構成を示すブロック

図である。記録再生装置100は、入出力I/F(Interface)120、MPEG(Moving Picture Experts Group)コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F(Interface)140、暗号処理手段150、ROM(Read Only Memory)160、CPU(Central Processing Unit)170、メモリ180、記録媒体195の記録媒体インタフェース(I/F)190を有し、これらはバス110によって相互に接続されている。

入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段150は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、又は復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU170は、メモリ180に記憶されたプログラムを実行するこ

とで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。記録媒体インタフェース190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し（再生し）、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。なお、プログラムをROM160に、デバイスキーをメモリ180に記憶する構成としてもよい。

モデム200は、電話回線を介して外部の装置と接続する。例えば、インターネット・サービス・プロバイダ（ISP：Internet Service Provider）のサーバと接続し、インターネット上のコンテンツ配信サーバなどとの通信路を確立する。

記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリなど、デジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

次に、図1の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図2A、図2B及び図3A、図3Bのフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図2Aのフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS201において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、暗号処理手段150に出力する。

暗号処理手段150は、ステップS202において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、記録媒体I/F190に出力する。暗号化コンテンツは、記録媒体I/F190を介して記録媒体195に記録（S203）され、記録処理

を終了する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP (Five Company Digital Transmission Content Protection) (以下、適宜、DTCPという) が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ (暗号化コンテンツ) を復号するようになっている。

このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS201で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。なお、DTCPの規格書は、DTLA (Digital Transmission Licensing Administrator) からインフォメーションバージョン (Informational Version) を誰でも取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図2Bのフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F140に供給されると、入出力I/F140は、ステップS221において、そのアナログコンテンツを受信し、ステップS222に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ（デジタルコンテンツ）とする。

このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS223において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

以下、ステップS224、S225において、図2AのステップS202、S203における処理と同様の処理が行われる。すなわち、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

次に、記録媒体195に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図3A及び図3Bのフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図3Aのフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップS301において、記録媒体I/F190によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

暗号処理手段150では、ステップS302において、記録媒体I/F190から供給される暗号化コンテンツが復号処理され、復号データがバス110を介して、入出力I/F120に供給される。ステップS303において、入出力I/F120はデジタルコンテンツを、外部に出力し、再生処理を終了する。

なお、入出力I/F120は、ステップS303で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCFの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとし

て外部に出力する場合においては、図3Bのフローチャートに従った再生処理が行われる。

即ち、ステップS321、S322において、図3AのステップS301、S302における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段I50において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

MPEGコーデック130では、ステップS323において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS324において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換して、アナログコンテンツとする。そして、ステップS325に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

次に、図1に示した記録再生装置が、データを記録媒体に記録、若しくは記録媒体から再生する際に必要なキー、例えばマスターキー若しくはメディアキーを、各機器に配布する構成について説明する。ここで、マスターキーは、このシステムにおいて共通で、複数のデバイスにおいて共通に保持されるキーであり、デバイスの製造時にデバイス内に記録される。このキー配信システムを用いるデバイス全てにおいて共通であることが望ましい。また、メディアキーは、各記録媒体に固有のキーであり、記録媒体の製造時に記録媒体に記録される。理想的には全ての記録媒体毎に異なるキーであることが望ましいが、記録媒体の製造工程の制約上、複数の記録媒体を1グループとして、グループ毎に変えることが現実的である。例えば、記録媒体の製造ロットを1グループとして、ロット毎にメディアキーを変えるように構成してもよい。以下においては、これらのキーを更新する例を中心に述べるが、マスターキーが記録されていないデバイス若しくはメディアキーが記録されていない記録媒体に、それぞれのキーを配布及び記録するために本発明を用いることもできる。

図4は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図4の最下段に示すナンバ0～15が個々の記録再生装置であ

る。すなわち図4に示す木（ツリー）構造の各葉（リーフ：leaf）がそれぞれの記録再生装置に相当する。

各デバイス0～15は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーを自身に格納する。図4の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

図4に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図4のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図4のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図4に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一

括してデータを送付する処理を実行する。このようなグループは、図4のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図4から明らかなように、1つのグループに含まれる4つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0, 1, 2, 3のみに提供することが可能となる。例えば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー：Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

また、ある時点tにおいて、デバイス3の所有する鍵：K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図5Aに示す

キー更新ブロック (KRB: Key Renewal Block) と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス 0, 1, 2 に供給することによって実行される。

図 5 A に示すキー更新ブロック (KRB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 5 A 及び図 5 B の例は、図 4 に示すツリー構造中のデバイス 0, 1, 2 において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図 4 から明らかなように、デバイス 0, デバイス 1 は、更新ノードキーとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス 2 は、更新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

図 5 A の KRB に示されるように KRB には複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス 2 の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図 5 A の下から 2 段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図 5 A の上から 2 段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図 5 A の上から 1 段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス 0, 1 は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス 0, 1 は、図 5 A の上から 3 段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図 5 A の上から 2 段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図 5 A の上から 1 段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 $K(t)R$ を得ることができる。なお、図 5 A のインデックスは、復号キー

として使用するノードキー、リーフキーの絶対番地を示す。

図4に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図5Bのキー更新ブロック（ KRB ：Key Renewal Block）を用いることで、更新ノードキー $K(t)00$ をデバイス0，1，2に配布することができる。

図5Bに示す KRB は、例えば特定のグループにおいて共有する新たなマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図4に点線で示すグループ内のデバイス0，1，2，3がある記録媒体を用いており、新たな共通のマスターキー $K(t)master$ が必要であるとする。このとき、デバイス0，1，2，3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新マスターキー： $K(t)master$ を暗号化したデータ $Enc(K(t), K(t)master)$ を図5Bに示す KRB とともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

すなわち、デバイス0，1，2，3は KRB を処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点でのマスターキー： $K(t)master$ やメディアキー： $K(t)media$ を得ることが可能になる。

図6に、本出願人の先の特許出願である特願2000-105328で提案した t 時点でのメディアキー $K(t)media$ を得る処理例として、 $K(t)00$ を用いて新たな共通のメディアキー $K(t)media$ を暗号化したデータ $Enc(K(t)00, K(t)media)$ と図5Bに示す KRB とを記録媒体を介して受領したデバイス2の処理を示す。

図4に示すように、ある記録再生システムには、点線で囲まれた、デバイス0，1，2，3の4つの装置が含まれるとする。図6は、デバイス3がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置（デバイス2）が記録媒体上のコンテンツを暗号化若しくは復号するために必要なメディアキーを、記録媒体に格納されている KRB （Key Renewal Block）と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表してい

る。

デバイス2のメモリには、自分にのみ割り当てられたリーフキーK0010と、そこから木のルートまでの各ノード001,00,0,Rのノードキー（それぞれ、K001,K00,K0,KR）が安全に格納されている。デバイス2は、図6の記録媒体に格納されているKRBのうち、インデックス（index）が0010の暗号文を自分の持つリーフキーK0010で復号してノード001のノードキーK

(t)001を計算し、次にそれを用いてインデックス（index）が001の暗号文を復号してノード00のノードキーK(t)_00を計算し、最後にそれを用いて暗号文を復号してメディアキーK(t)_mediaを計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

図7の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理及び記録媒体に対する記録処理の一例について説明する。

記録再生装置700は自身の上述したKRBに基づく算出処理によってメディアキーを取得する。

次に、記録再生装置700は例えば光ディスクである記録媒体702に識別情報としてのディスクID（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、ディスクID（Disc ID）を読出し、記録されていなければ、暗号処理手段150においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法でディスクID（Disc ID）1701を生成し、ディスクに記録する。ディスクID（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器700は、次にメディアキー701とディスクIDを用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図8に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクID（Disc ID）を入力して得られた結果を用いる例1の方法や、FIPS（Federal Information Processing Standards

Publications) 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例2の方法が適用できる。

次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1参照) においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク702に記録する。

次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイスID、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キー、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

このタイトル固有キー (Title Unique Key) 生成の具体的な方法は、図9に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、デバイスID (再生機器制限をしない場合) 若しくはデバイス固有キー (再生機器制限をする場合) を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とデバイスID (再生機器制限をしない場合) 若しくはデバイス固有キー (再生機器制限をする場合) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。なお、再生機器制限とは、記録媒体に格納されたコンテンツデータを制限された特定の再生機器においてのみ再生可能とすることを意味する。

なお、上記の説明では、メディアキーとディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイスID、若しくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキーとディスクID (Disc ID) とタイトルキー (Title Key) と、デバイスID若しくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイ

トルキー (Title Key) を用いずに、メディアキー (Master Key) とディスク ID (Disc ID) と、デバイス ID 若しくはデバイス固有キーからタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

さらに、図 7 を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第 1~4 バイトが分離されて出力されるブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロックキー (Block Key) が生成される。

ブロックキー (Block Key) の生成方法の例を図 10 に示す。図 10 では、いずれも 32 ビットのブロックシード (Block Seed) と、64 ビットのタイトル固有キー (Title Unique Key) とから、64 ビットのブロックキー (Block Key) を生成する例を 2 つ示している。

上段に示す例 1 は、鍵長 64 ビット、入出力がそれぞれ 64 ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と 32 ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

例 2 は、FIPS 180-1 のハッシュ関数 SHA-1 を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値を SHA-1 に入力し、その 160 ビットの出力を、例えば下位 64 ビットのみ使用するなど、64 ビットに縮約したものをブロックキー (Block Key) としている。

なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、例えば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにメディアキーとディスク ID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、デバイス ID、若しくはデバイス固有キーを用いてブロックキー (Block Key) を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図 7 の下段に示すように、ブロックシード (Block

k.Seed)を含むブロックデータの先頭の第1~mバイト(例えばm=8バイト)は分離(セクタ1608)されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブロック・シードとしての第1~4バイトも含まれる。セクタにより分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるDES(Data Encryption Standard)を用いることができる。

以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロックシード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

記録媒体に格納された暗号化コンテンツデータの復号及び再生処理を説明するブロック図11に示す。

再生処理においては、図7~図10を用いて説明した暗号化及び記録処理と同様、メディアキーとディスクIDからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体702から読み取られるブロック単位の暗号化データの復号処理を実行する。

上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、及び記録媒体からの再生時の復号処理においては、KRBに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、又は復号処理用の鍵を生成する。

なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーをKRBから取得して、これらに基づいてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成としてもよい。さらに、KRBから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、及び復号処理に用いるキーとして適用することも可能であ

る。

いずれの構成においても、デバイスは、データの記録、再生時において、図6の記録媒体に格納されているKRBに基づく複数回の復号処理により、データの暗号化又は復号に必要な暗号化キー又は該暗号化キー生成用データを算出することが要請される。このKRB処理に要する計算回数は、前述したように、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。

これらの処理を軽減する本発明における記録再生装置のメディアキーの取り扱い構成を説明する図を図12に示す。本発明の構成では、ある記録媒体に格納されているKRBから、記録再生装置がメディアキーを計算するところまでは、図6の処理と同様であるが、本発明においては、メディアキーを自分だけが知る鍵、情報記録再生装置固有のキー、例えば本構造において自分だけに割り当てられているリーフキーを用いて暗号化し、あらかじめ記録媒体に用意されている領域に、記録再生装置の識別情報、例えばその記録再生装置に割り当てられたリーフ番号とともに記録する構成とした。図12のデバイス2は、KRBの処理によって取得したメディアキー $K(t)_{media}$ を自身の有するリーフキー $K0010$ で暗号化して、記録媒体に格納する。

このように、KRBの複数段の復号処理により取得したメディアキーを再度使用する際に、新たに複数段の復号処理を実行することなく、簡単な復号処理のみで取得可能となる。すなわち、同一の記録再生装置がこの記録媒体を2度目以降にアクセスする際には、わざわざKRBを用いて大量の計算を行わなくても、メディアキー格納テーブルに格納されている暗号文を自分の固有鍵で復号することによってメディアキーを得ることが可能となる。また、記録デバイスに格納された暗号化メディアキーは、デバイス2に固有のリーフキーによってのみ復号可能であるので、他のデバイスに記録媒体を装着しても、暗号化メディアキーを復号して取得することはできない。

本発明における記録再生装置が、記録媒体にアクセスする際、すなわち、例えば記録媒体が記録再生装置に装着された際にメディアキーを得るフローを図13

に示す。図13の処理フローについて説明する。

ステップS1301において、記録再生装置は記録媒体に記録されているメディアキー格納テーブルを読み出す。S1302で、メディアキー格納テーブルのインデックス部を見て、自分自身に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければS1303に進み、あればS1309に進む。

S1303では、記録再生装置は、記録媒体から、KRB (Key Renewal Block) を読み出す。ステップS1304において、記録再生装置は、ステップS1303で読み出したKRBと、自身がメモリに格納しているリーフキー (図4のデバイス2におけるK0010) 及びノードキー (図4のデバイス2におけるK001, K00...) を用いて、識別番号: 世代 (Generation) (図7におけるt) のKRBにおけるノード00の鍵K(t)00を計算する。

ステップS1305で、記録媒体からEnc(K(t)00, K(t)media)、すなわち、K(t)00を用いてメディアキーK(t)mediaを暗号化した値を読み出す。

そしてステップS1306において、この暗号文をK(t)00を用いて復号してK(t)mediaを計算する。このようにして計算したメディアキーは、その記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

また、ステップS1307では、自身のみが持つリーフキー (図4のデバイス2におけるK0010) を用いてメディアキーK(t)mediaを暗号化する。

ステップS1308において、S1307で作成した暗号文と、自身の識別情報となる、リーフキーの番号 (リーフ番号) 0010を、記録媒体のメディアキー格納テーブルに記録し、処理を終了する。

ステップS1302において、自身が格納した暗号文がメディアキー格納テーブルに見つかった場合には、S1309に進み、記録再生装置は記録媒体からその暗号文を読み出す。

S1310において、自身のリーフキーを用いてその暗号文を復号することにより、その記録媒体のメディアキーを得る。これをその記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

なお、上記の処理において、ステップS1307及びS1308の処理は、記録媒体のメディアキー格納テーブルに、新たに一組のインデックス(index)と暗号文を書きこめる場合のみ行う、図14のようにすることも可能である。

図14において、S1301乃至S1306及びS1307乃至S1310は、それぞれ図13の同ステップと同様であるので説明は省略する。

ステップS1401において、記録再生装置は記録媒体のメディアキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、ステップS1307に進み、S1308において暗号文をテーブルに記録するが、スペースが残っていなければ、S1307及びS1308の処理をスキップして終了する。

上述の実施例においては、先の図12を用いて説明したように、記録媒体に個々の記録再生装置が用いるテーブルを置いたが、本実施例においては、図15に示すように、個々の記録再生装置内に記憶手段、例えば図1に示す記録再生装置100のメモリ180に、記録媒体ごとのメディアキーを格納する。

記録再生装置100のメモリ180に暗号化処理を施したメディアキーを格納する格納態様は、メディアキーの世代情報をインデックスとして、暗号化処理を施したメディアキーを対応付けたメディアキー格納テーブル構成としている。複数の異なる世代のメディアキーを格納する場合を考慮した構成としている。

上述の実施例と同様の前提において、本実施例における記録再生装置が、記録媒体にアクセスする際、すなわち、例えば記録媒体が記録再生装置に装着された際にメディアキーを得るフローを図16に示す。

ステップS1601において、記録再生装置は記録媒体からそこに格納されているKRB及びメディアキーの識別番号である世代(Generation)(図15の例ではt)を読み出す。

S1602において、記録再生装置は自身内部に格納しているメディアキー格納テーブルにもという世代(Generation)を持つメディアキーが格納されているかどうかを検査する。格納されていなければS1603に進み、格納されていればS1610に進む。

S1603乃至S1606の処理は、それぞれ図13のS1303乃至S13

06の各処理と同様であるので説明を省略するが、これらの処理の結果、記録再生機器はメディアキーを得る。このようにして計算したメディアキーは、その記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

S1607において、記録再生機器は自身の記録手段のメディアキー格納テーブルに新たにメディアキーを格納するスペースがあるかどうかを確認する。スペースがあればS1608に進み、なければS1608及びS1609の処理をスキップする。

S1608では、図13のS1307と同様に、自身のリーフキーを用いてメディアキーを暗号化する。S1609で、上記暗号文を、識別情報：世代 (Generation) とともにメディアキー格納テーブルに格納する。

ステップS1602において、世代 (Generation) に対応した暗号文がメディアキー格納テーブルに見つかった場合には、S1610に進み、記録再生装置はメディアキー格納テーブルからその暗号文を読み出す。S1611において、図13のS1310と同様に、自身のリーフキーを用いてその暗号文を復号することにより、その記録媒体のメディアキーを得る。これをその記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

なお、上記の実施例においては、メディアキー格納テーブルにメディアキーを格納する際に、自身のリーフキーを用いて暗号化するようにしているが、例えばメディアキー格納テーブルの内容が外部に露呈することがなく、安全な記録が行える場合には、必ずしも暗号化は必要ではない。すなわち、図17のように、KRBの復号処理によって得られるメディアキー $K(t)_{media}$ をそのまま、暗号化せずに、インデックスとしての世代 (Generation) に対応させて格納する構成としてもよい。この場合は、メディアキー $K(t)_{media}$ を再度使用する場合は、復号処理が不要となる。

また、上述の実施例を組み合わせ、メディアキー格納テーブルを記録媒体と記録再生装置の両方に持たせるようにすることも可能である。

なお、上述の例では、KRB処理に基づいて取得するキーをメディアキーとして説明したが、この方法は、メディアキーに特化したものではなく、例えば複数のデバイスに共通に格納されたマスターキー、デバイス毎に固有のデバイスキー

に適用することももちろん可能である。

なお、上述の例では、鍵を配信するためのデータをキー更新ブロック (KR B) という表現を用いて説明したが、キー更新ブロックは、鍵の更新に限られるものではなく、鍵の配布全般に適応可能であることは、上述の説明から明らかである。

次に、図1に示した記録再生装置が、データを記録媒体に記録、若しくは記録媒体から再生する際に必要なキー、例えばコンテンツキーを、各機器に配布する構成について説明する。ここで、コンテンツキーは、通信媒体若しくは記録媒体を介して配布される暗号化されたコンテンツを復号するための鍵である。図18は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図18の最下段に示すナンバ0～15が個々の記録再生装置である。すなわち図18に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

各デバイス0～15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)及び各リーフのリーフキーを自身に格納する。図18の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR～K111をノードキーとする。

図18に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー: K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図18のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図18のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存

することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図18に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図18の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、コンテンツキーを暗号化して送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図18の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図18のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図18から明らかなように、1つのグループに含まれる4つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通の暗号化コンテンツキーをデバイス0, 1, 2, 3のみに提供することが可能となる。例えば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKcontentをノードキーK00で暗号化した値Enc(K00, Kcontent)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcontent)を解いてコンテンツキー: K

contentを得ることが可能となる。なお、 $Enc(K_a, K_b)$ は K_b を K_a によって暗号化したデータであることを示す。

また、ある時点 t において、デバイス3の所有する鍵： $K0011, K001, K00, K0, KR$ が攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー： $K001, K00, K0, KR$ をそれぞれ新たな鍵 $K(t)001, K(t)00, K(t)0, K(t)R$ に更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、 $K(t)aaa$ は、鍵 $Kaaa$ の世代（Generation）： t の更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図19Aに示すキー更新ブロック（ KRB ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納して、デバイス0, 1, 2に供給することによって実行される。

図19Aに示すキー更新ブロック（ KRB ）には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図19Aの例は、図18に示すツリー構造中のデバイス0, 1, 2において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図18から明らかなように、デバイス0, デバイス1は、更新ノードキーとして $K(t)00, K(t)0, K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001, K(t)00, K(t)0, K(t)R$ が必要である。

図19Aの KRB に示されるように KRB には複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図19Aの下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得る

ことができる。以下順次、図19Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図19Aの上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス0, 1は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス0, 1は、図19Aの上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図19Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図19Aの上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0, 1, 2は更新した鍵 $K(t)R$ を得ることができる。なお、図19Aのインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。図18に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図19Bのキー更新ブロック(KRB: Key Renewal Block)を用いることで、更新ノードキー $K(t)00$ をデバイス0, 1, 2に配布することができる。

図19Bに示すKRBは、例えば特定のグループにおいて共有するコンテンツキー、又はマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図18に点線で示すグループ内のデバイス0, 1, 2, 3にコンテンツキーで暗号化したコンテンツを提供するとともに、暗号化処理したコンテンツキー $K(s)content$ を提供する必要があるとする。ここで s は、コンテンツを識別するためのコンテンツIDを示す。このとき、デバイス0, 1, 2, 3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて共通のコンテンツキー： $K(s)content$ を暗号化したデータ $Enc(K(t), K(s)content)$ を図19Bに示すKRBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキー等、各種キーについても同様である。

すなわち、デバイス0, 1, 2, 3はKRBを処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点でのコンテンツキー： $K(s)content$ やメ

ディアキー: $K(t) \text{ media}$ を得ることが可能になる。

上述のキー配信構成としてのツリー構造の各リーフに配置された情報記録再生装置に対して音楽データなどのコンテンツをコンテンツキーで暗号化して提供する場合、そのデータ構成は、図20に示す形態となる。

図20に示すように、データは、鍵配信部と、コンテンツデータ部とから構成される。鍵配信部は、上述したキー更新ブロック (KRB: Key Renewal Block) を有し、さらに、キー更新ブロック (KRB) の処理によって得られる更新ノードキーによって暗号化されたコンテンツキー: $K(s) \text{ content}$ を含む構成となっている。コンテンツデータ部は、コンテンツキー: $K(s) \text{ content}$ によって暗号化されたコンテンツ: $\text{Enc}(K(s) \text{ content}, \text{Content})$ が格納されている。

前述したようにキー更新ブロック (KRB) の処理によって更新ノードキーを取得可能な情報記録再生装置は様々に設定することが可能であり、図20のような暗号化コンテンツの提供構成をとることにより、特定の情報処理装置のみが復号可能なコンテンツを提供することが可能となる。

図21に、本出願人の先の特許出願である特願2000-105329で提案したコンテンツID=sのコンテンツキー $K(s) \text{ content}$ により暗号化されたコンテンツを利用する処理例として、KRBをK0010を用いて処理し、コンテンツキー $K(s) \text{ content}$ を取得して、暗号化したデータ $\text{Enc}(K(s) \text{ content}, \text{content})$ からコンテンツを取得するデバイス2の処理を示す。

図18に示すように、ある記録再生システムには、点線で囲まれた、デバイス0, 1, 2, 3の4つの装置が含まれるとする。図21は、デバイス3がリボークされた状態で、コンテンツキー $K(s) \text{ content}$ を使用する場合に、記録再生装置 (デバイス2) において受領するデータの処理を示している。すなわち、コンテンツキー $K(s) \text{ content}$ を、記録媒体に格納されているKRB (Key Renewal Block) に基づいて求める際の処理を表している。

デバイス2のメモリには、自分にのみ割り当てられたリーフキーK0010と、そこから木のルートまでの各ノード001, 00, 0, Rのノードキー (それぞれ、K001, K00, K0, KR) が安全に格納されている。デバイス2は、図21の

記録媒体に格納されているKRBのうち、インデックス(index)が0010の暗号文を自分の持つリーフキーK0010で復号してノード001のノードキーK(t)001を計算し、次にそれを用いてインデックス(index)が001の暗号文を復号してノード00のノードキーK(t)00を計算し、次にそれを用いてインデックス(index)が00の暗号文を復号してノード0のノードキーK(t)0計算し、最後にそれを用いてインデックス(index)が0の暗号文を復号してノードRのノードキーK(t)Rを計算し、さらに、ノードキーK(t)Rを用いて、 $Enc(K(t)R, K(s)content)$ を解いてコンテンツID=sのコンテンツキーK(s)contentを取得する。

その取得したコンテンツキーK(s)contentを用いてコンテンツデータ部に格納された暗号化コンテンツ： $Enc(K(s)content, Content)$ を復号してコンテンツを得る。

このような処理ステップをすべて実行することにより、暗号化コンテンツの復号処理が可能となる。上述のようにキー更新ブロック(KRB)の処理によって更新ノードキーを取得する処理は、繰り返し同様の復号処理を実行することが必要であり、この計算回数は、リーフからコンテンツキーを暗号化したノードキーまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。

情報記録再生装置は、コンテンツの再生時において、例えば記録媒体に格納されているKRBに基づく複数回の復号処理により、コンテンツキーを算出することが要請される。例えばコンテンツキーが、コンテンツ毎に異なる鍵として設定されている場合には、それぞれのコンテンツの再生毎に上述のKRB処理を実行することが必要になる。

これらの処理を軽減する本発明における記録再生装置のコンテンツキーの取り扱い構成を説明する図を図22に示す。本発明の構成では、ある記録媒体に格納されているKRBから、記録再生装置がコンテンツキーを計算するところまでは、図21の処理と同様であるが、本発明においては、コンテンツキーを自分だけが知る鍵、すなわち情報記録再生装置固有のキー、例えば木構造において自分だけに割り当てられているリーフキーを用いて暗号化し、例えばあらかじめ記録媒体

に用意されている領域に、記録再生装置の固有キー識別情報、例えばその記録再生装置に割り当てられたリーフ番号とともに記録する構成とした。例えば図22に示すようにデバイス2の場合、リーフキーを用いて暗号化したコンテンツキー：Enc(K0010, K(s) content)は、図22に示すように、コンテンツキー格納テーブルとして、対応コンテンツと組にして記録媒体に格納する。

このようなコンテンツキー格納テーブルの格納構成を採用することにより、KRBの複数段の復号処理により取得したコンテンツキーを再度使用する際、新たに複数段の復号処理を実行することなく、簡単な復号処理のみでコンテンツキーを取得することが可能となる。すなわち、同一の記録再生装置がこの記録媒体を2度目以降にアクセスする際には、わざわざKRBを用いて大量の計算を行わなくても、コンテンツキー格納テーブルに格納している暗号文を自分の固有鍵で復号することによってコンテンツキーを得ることが可能となる。また、デバイスに格納された暗号化コンテンツキーは、そのデバイスに固有のリーフキーによってのみ復号可能であるので、他のデバイスに記録媒体を装着しても、暗号化コンテンツキーを復号して取得することはできない。

本発明における記録再生装置が、コンテンツを利用する際、すなわち、例えば記録媒体が記録再生装置に装着され、暗号化コンテンツキーを取得してコンテンツを復号、再生する処理を示すフローを図23に示す。図23の処理フローについて説明する。以下は、記録媒体からのコンテンツの再生に関して説明を行うが、通信媒体からコンテンツを取得する場合であっても同様である。

ステップS701において、記録再生装置は記録媒体に記録されているコンテンツと一緒に記録されているコンテンツキー格納テーブルを読み出す。

ステップS702で、コンテンツキー格納テーブルのインデックス部を見て、自分自信に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければS703に進み、あればS710に進む。

S703では、記録再生装置は、記録媒体からKRB(Key Renewal Block)を読み出す。ステップS704において、記録再生装置は、ステップS703で読み出したKRBと、自身がメモリに格納しているリーフキー(図18のデバイス

2においては、K 0 0 1 0) 及びノードキー (図 1 8 のデバイス 2 においては、K 0 0 1, K 0 0 ...) を用いて、現在自身が再生しようとしているコンテンツの識別番号: コンテンツ ID (図 2 2 における t_s) の K R B におけるノード R の鍵、すなわちルートキー $K(t)R$ を計算する。なお、この例では、ルートキー $K(t)R$ により、コンテンツキーが暗号化されて提供されている例を示しているが、ルートキーより下位のノードキーを用いて、更新ノードキー $K(t)xx$ を設定し、その更新ノードキー $K(t)xx$ によりコンテンツキーを暗号化して、特定のグループにのみ復号可能なコンテンツキーを配布する構成とした場合は、その更新ノードキーを計算によって算出する。

ステップ S 7 0 5 で、記録媒体から $Enc(K(t)R, K(s)content)$ 、すなわち、 $K(t)R$ を用いてコンテンツキー $K(s)content$ を暗号化した値を読み出す。

そしてステップ S 7 0 6 において、この暗号文を $K(t)R$ を用いて復号して $K(s)content$ を計算する。ステップ S 7 0 7 では、記録再生装置は記録媒体上のそのコンテンツのコンテンツキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、S 7 0 8 に進み、スペースが残っていなければ、S 7 0 8 及び S 7 0 9 の処理をスキップして S 7 1 2 に進む。

ステップ S 7 0 8 では、自身のみが持つリーフキー (例えば、図 1 8 のデバイス 2 においては、K 0 0 1 0) を用いてコンテンツキー $K(s)content$ を暗号化する。

ステップ S 7 0 9 において、S 7 0 8 で作成した暗号文と、自身の識別情報となるリーフキーの番号 (リーフ番号) 0 0 1 0 (図 1 8 のデバイス 2 の場合) を、記録媒体のコンテンツキー格納テーブルに記録し、ステップ S 7 1 2 に進む。

一方、ステップ S 7 0 2 において、自身が格納した暗号文がコンテンツキー格納テーブルに見つかった場合には、S 7 1 0 に進み、記録再生装置は記録媒体からその暗号文を読み出す。

S 7 1 1 において、自身のリーフキーを用いてその暗号文を復号することにより、そのコンテンツのコンテンツキーを得て、ステップ S 7 1 2 に進む。ステッ

ブ S 7 1 2 では、記録媒体からコンテンツデータ部を読み出し、S 7 0 6 又は S 7 1 1 で得たコンテンツキーを用いて復号することにより平文データを得て、利用する。

このようにすることにより、記録再生機器が、コンテンツを利用するたびに K R B を用いてコンテンツキーを計算する処理を大幅に減少させることが可能となる。

コンテンツを記録媒体に記録する際は、通信媒体又は記録媒体を介して伝送あるいは供給された図 2 0 に示すコンテンツ、すなわちコンテンツデータ部と、鍵配信部を単に記録媒体に記録する。この際に、コンテンツ再生処理と同様、図 2 3 の S 7 0 1 ~ S 7 0 9 の処理を行なう。この処理フローを図 2 4 に示す。

図 2 4 のコンテンツ記録時の処理においては、図 2 3 のコンテンツ再生時の処理とほぼ同様の処理が実行される。ステップ S 8 0 1 において、記録再生装置は記録媒体に記録されているコンテンツキー格納テーブルを読み出す。

ステップ S 8 0 2 で、コンテンツキー格納テーブルのインデックス部を見て、自分自身に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければ S 8 0 3 に進み、あれば S 8 1 2 に進む。

S 8 0 3 では、記録再生装置は、記録媒体から、K R B (Key Renewal Block) を読み出す。ステップ S 8 0 4 において、記録再生装置は、ステップ S 8 0 3 で読み出した K R B と、自身がメモリに格納しているリーフキー (図 1 8 のデバイス 2 における K 0 0 1 0) 及びノードキー (図 1 8 のデバイス 2 における K 0 0 1, K 0 0 ...) を用いて、コンテンツの識別番号: コンテンツ ID (図 2 2 における s) の K R B におけるノード R の鍵、すなわちルートキー K (t) R を計算する。

ステップ S 8 0 5 で、記録媒体から E n c (K (t) R, K (s) content)、すなわち、K (t) R を用いてコンテンツキー K (s) content を暗号化した値を読み出す。

そしてステップ S 8 0 6 において、この暗号文を K (t) R を用いて復号して K (s) content を計算する。ステップ S 8 0 7 では、記録再生装置は記録媒体上

のそのコンテンツのコンテンツキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、S 8 0 8に進み、スペースが残っていなければ、S 8 0 8及びS 8 0 9の処理をスキップしてS 8 1 2に進む。

また、ステップS 8 0 8では、自身のみが持つリーフキー（例えば図18のデバイス2においては、K 0 0 1 0）を用いてコンテンツキーK (s) contentを暗号化する。

ステップS 8 0 9において、S 8 0 8で作成した暗号文と、自身の識別情報となる、リーフキーの番号0 0 1 0（図18のデバイス2の場合）を、記録媒体のコンテンツキー格納テーブルに記録し、ステップS 8 1 2に進む。

一方、ステップS 8 0 2において、自身が格納した暗号文がコンテンツキー格納テーブルに見つかった場合には、S 8 0 3～S 8 0 9をスキップしてS 8 1 2に進む。

ステップS 8 1 2では、通信媒体又は記録媒体を介して伝送あるいは供給されたコンテンツ、すなわちコンテンツキーK (s) contentで暗号化されているコンテンツデータ部と、鍵配信部を、そのまま記録媒体に格納する。なお、この例では、コンテンツの格納を最後にしているが、コンテンツはあらかじめ図20に示すように暗号化されているものであり、S 8 0 1の前にコンテンツ記録媒体に格納してもよく、コンテンツ格納処理はいつ実行してもよい。

このようにデータ記録時のコンテンツキーを自身の装置固有のキー、例えばリーフキーによって暗号化して記録媒体に格納することにより、その後、記録再生機器がコンテンツを利用する際にK R Bを用いてコンテンツキーを計算する処理を大幅に減少させることが可能となる。

上述の実施例においては、先の図22を用いて説明したように、個々の記録再生装置が用いるコンテンツキー格納テーブルを記録媒体上にコンテンツとともに置いたが、本実施例においては、図25に示すように、個々の記録再生装置内に記憶手段、例えば図1に示す記録再生装置100のメモリ180に、コンテンツキーを格納する。

記録再生装置100のメモリ180に暗号化処理を施したコンテンツキーを格

納する格納態様は、コンテンツキーのコンテンツIDをインデックスとして、暗号化処理を施したコンテンツキーを対応付けたコンテンツキー格納テーブル構成としている。複数の異なるコンテンツIDのコンテンツキーを格納する場合を考慮した構成としている。

上述の実施例と同様の前提において、本実施例における記録再生装置が、コンテンツを利用する際、すなわち、例えば暗号化コンテンツが格納された記録媒体が記録再生装置に装着され、暗号化コンテンツを復号して再生するフローを図26に示す。

ステップS1001において、記録再生装置は記録媒体から、自身が再生しようとしているコンテンツの識別番号であるコンテンツID (Content ID) (図25の例ではs) を読み出す。

S1002において、記録再生装置は記録装置自身の内部に格納しているコンテンツキー格納テーブルにsというコンテンツIDを持つコンテンツキーが格納されているかどうかを検査する。格納されていなければS1003に進み、格納されていればS1010に進む。

S1003乃至S1006の処理は、それぞれ図23のS703乃至S706の各処理と同様であるので説明を省略するが、これらの処理の結果、記録再生機器はコンテンツキーを得る。

S1007において、記録再生機器は自身の記録手段のコンテンツキー格納テーブルに新たにコンテンツキーを格納するスペースがあるかどうかを確認する。スペースがあればS1008に進み、なければS1008及びS1009の処理をスキップする。

S1008では、図23のS708と同様に、自身のリーフキーを用いてコンテンツキーを暗号化する。S1009で、上記暗号文を、識別情報であるコンテンツIDとともにコンテンツキー格納テーブルに格納し、ステップS1012に進む。

ステップS1002において、コンテンツIDに対応した暗号文がコンテンツキー格納テーブルに見つかった場合には、S1010に進み、記録再生装置はコンテンツキー格納テーブルからその暗号文を読み出す。S1011において、図

23のS711と同様に、自身のリーフキーを用いてその暗号文を復号することにより、そのコンテンツのコンテンツキーを得て、ステップS1012に進む。

ステップS1012では、図23のS712と同様に、記録媒体からコンテンツデータ部を読み出し、S1006又はS1011で得たコンテンツキーを用いて暗号化コンテンツの復号処理を実行して、音楽データ等のコンテンツの平文データを得て、再生利用する。

なお、上記の実施例においては、コンテンツキー格納テーブルにコンテンツキーを格納する際に、自身のリーフキーを用いて暗号化するようにしているが、例えばコンテンツキー格納テーブルの内容が外部に露呈することがなく、安全な記録が行える場合には、必ずしも暗号化は必要ではない。また、上記の例では、コンテンツを利用する際にコンテンツキー格納テーブルに自身のリーフキーで暗号化したコンテンツキーを格納するようにしているが、コンテンツを記録媒体に記録する際、すなわち、コンテンツキーを用いてコンテンツを暗号化して記録媒体に格納し、その暗号化に用いたコンテンツキーを上述と同様にコンテンツキー格納テーブルに格納する処理を行う構成としてもよい。

また、上述の実施例を組み合わせ、コンテンツキー格納テーブルを記録媒体と記録再生装置の両方に持たせるようにすることも可能である。

なお、上述の例では、鍵を配信するためのデータをキー更新ブロック（KRB）という表現を用いて説明したが、キー更新ブロックは、鍵の更新に限られるものではなく、鍵の配布全般に適応可能であることは、上述の説明から明らかである。

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録

再生を行う場合の図 1 の記録再生装置の処理について、図 2 7 A、図 2 7 B 及び図 2 8 A、図 2 8 B のフローチャートを参照して説明する。

まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図 2 7 A のフローチャートにしたがった記録処理が行われる。図 2 7 A の処理について説明する。ここでは、図 1 の記録再生器 1 0 0 を例として説明する。デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE 1394 シリアルバス等を介して、入出力 I / F 1 2 0 に供給されると、ステップ S 1 8 0 1 において、入出力 I / F 1 2 0 は、そのデジタルコンテンツを受信し、ステップ S 1 8 0 2 に進む。

ステップ S 1 8 0 2 では、入出力 I / F 1 2 0 は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力 I / F 1 2 0 が受信したコンテンツが暗号化されていない場合（例えば、上述の D T C P を使用せずに、平文のコンテンツが、入出力 I / F 1 2 0 に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置 1 0 0 が D T C P に準拠している装置であるとし、D T C P に従って処理を実行するものとする。D T C P では、コピーを制御するためのコピー制御情報としての 2 ビットの E M I (Encryption Mode Indicator) が規定されている。E M I が 0 0 B (B は、その前の値が 2 進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-freely) であることを表し、E M I が 0 1 B である場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、E M I が 1 0 B である場合は、コンテンツが、1 度だけコピーして良いもの (Copy-one-generation) であることを表し、E M I が 1 1 B である場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であることを表す。

記録再生装置 1 0 0 の入出力 I / F 1 2 0 に供給される信号に E M I が含まれ、その E M I が、Copy-freely や Copy-one-generation であるときには、コンテンツはコピー可能であると判定される。また、E M I が、No-more-copies や Copy-never であるときには、コンテンツはコピー可能でないと判定される。

ステップ S 1 8 0 2 において、コンテンツがコピー可能でないと判定された場

合、ステップS 1 8 0 3～S 1 8 0 4をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体1 0に記録されない。

また、ステップS 1 8 0 2において、コンテンツがコピー可能であると判定された場合、ステップS 1 8 0 3に進み、以下、ステップS 1 8 0 3～S 1 8 0 4において、図2 AのステップS 2 0 2、S 2 0 3における処理と同様の処理が行われる。すなわち、暗号処理手段1 5 0における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体1 9 5に記録して、記録処理を終了する。

なお、EMIは、入出力I/F 1 2 0に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報（例えば、D T C Pにおけるembedded CCIなど）も記録される。

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図2 7 Bのフローチャートにしたがった記録処理が行われる。図2 7 Bの処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F 1 4 0に供給されると、入出力I/F 1 4 0は、ステップS 1 8 1 1において、そのアナログコンテンツを受信し、ステップS 1 8 1 2に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップS 1 8 1 2の判定処理は、例えば、入出力I/F 1 4 0で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F 1 4 0で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、CGMS-A信号は、ディジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-gen

eration)、又はコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

ステップS1812において、アナログコンテンツがコピー可能でないと判定された場合、ステップS1813乃至S1816をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体195に記録されない。

また、ステップS1812において、アナログコンテンツがコピー可能であると判定された場合、ステップS1813に進み、以下、ステップS1813乃至S1816において、図2BのステップS222乃至S225における処理と同様の処理が行われ、これにより、コンテンツがディジタル変換、MP EG符号化、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図28Aのフローチャートにしたがった再生処理が行われる。図28Aの処理について説明する。最初に、ステップS1901、S1902において、図3AのステップS301、S302における処理

と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段 150 において復号処理がなされ、復号処理が実行されたデジタルコンテンツは、バス 110 を介して、入出力 I/F 120 に供給される。

入出力 I/F 120 は、ステップ S 1903 において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力 I/F 120 に供給されるデジタルコンテンツに EMI、あるいは、EMI と同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力 I/F 120 に供給されるデジタルコンテンツに EMI 等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、D T C P の規格にしたがって、EMI が記録された場合には、その EMI（記録された EMI (Recorded EMI)）が、Copy-freely であるときには、コンテンツは、後でコピー可能なものであると判定される。また、EMI が、No-more-copies であるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録された EMI 等のコピー制御情報が、Copy-one-generation や Copy-never であることはない。Copy-one-generation の EMI は記録時に No-more-copies に変換され、また、Copy-never の EMI を持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいて例えば「Copy-one-generation のコピー制御情報は、No-more-copies に変換せずに記録するが、No-more-copies として扱う」などのルールが決められている場合は、この限りではない。

ステップ S 1903 において、コンテンツが、後でコピー可能なものであると判定された場合、ステップ S 1904 に進み、入出力 I/F 120 は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップ S 1903 において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップ S 1905 に進み、入出力 I/F 120 は、例えば、D T C P の規格等にしたがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（若しくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力I/F120は、DTCPの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTCPの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図28Bのフローチャートにしたがった再生処理が行われる。図28Bの処理について説明する。ステップS1911乃至S1914において、図3BのステップS321乃至S324における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

入出力I/F140は、ステップS1915において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMI等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えば、DTCPの規格にしたがって、EMI等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、EMI等のコピー制御情報が、No-more-copiesである場合、若しくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、アナログコンテンツは、後でコピー可能なものでないと

判定される。

さらに、例えば、入出力 I/F 140 に供給されるアナログコンテンツに CGMS-A 信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともに CGMS-A 信号が記録された場合には、その CGMS-A 信号が、Copy-freely であるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A 信号が、Copy-never であるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

ステップ S1915 において、コンテンツが、後でコピー可能であると判定された場合、ステップ S1916 に進み、入出力 I/F 140 は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップ S1915 において、コンテンツが、後でコピー可能でないと判定された場合、ステップ S1917 に進み、入出力 I/F 140 は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録された EMI 等のコピー制御情報が、No-more-copies である場合（若しくは、システムにおいて例えば「Copy-one-generation のコピー制御情報は、No-more-copies に変換せずに記録するが、No-more-copies として扱う」というルールが決められていて、その条件下で記録された EMI 等のコピー制御情報が Copy-one-generation である場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力 I/F 140 は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-never を表す CGMS-A 信号を付加して、外部に出力する。また、例えば、記録された CGMS-A 信号が、Copy-never である場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力 I/F 4 は、CGMS-A 信号を Copy-never に変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化／復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図29は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク2005やROM2003に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体2010に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体2010は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体2010からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部2008で受信し、内蔵するハードディスク2005にインストールすることができる。

コンピュータは、CPU(Central Processing Unit)2002を内蔵している。CPU2002には、バス2001を介して、入出力インタフェース2011が接続されており、CPU2002は、入出力インタフェース2010を介して、ユーザによって、キーボードやマウス等で構成される入力部2007が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)2003に格納されているプログラムを実行する。

あるいは、CPU 2002は、ハードディスク2005に格納されているプログラム、衛星若しくはネットワークから転送され、通信部2008で受信されてハードディスク2005にインストールされたプログラム、又はドライブ2009に装着されたリムーバブル記録媒体2010から読み出されてハードディスク2005にインストールされたプログラムを、RAM(Random Access Memory)2004にロードして実行する。

これにより、CPU 2002は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU 2002は、その処理結果を、必要に応じて、例えば、入出力インタフェース2011を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部2006から出力、あるいは、通信部2008から送信、さらには、ハードディスク2005に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理(例えば、並列処理あるいはオブジェクトによる処理)も含むものである。

また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

以上、説明したように、本発明の情報記録再生装置によれば、ツリー（木）構造の鍵配布構成により、コンテンツ暗号鍵としての例えばメディアキーの更新データを更新ブロック（KRB）とともに送信する構成とし、記録再生装置がある記録媒体のメディアキーを計算して取得した後に、取得したメディアキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する構成としたので、記録再生装置が、次にその記録媒体を使用する際に、その暗号化キーを1回復号するだけでメディアキーを計算できる。従って、記録再生装置が記録媒体にアクセスする際に必要となるKRB復号処理等の計算量を減少させることが可能となる。

また、ツリー（木）構造の鍵配布構成により、コンテンツ暗号鍵としてのコンテンツキーを更新ブロック（KRB）とともに送信する構成とし、記録再生装置があるコンテンツのコンテンツキーを計算して取得した後に、取得したコンテンツキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して暗号文を生成し、記録媒体、又は記録再生装置のメモリに格納する構成としたので、記録再生装置が、次にそのコンテンツを使用する際に、その暗号文を1回復号するだけでコンテンツキーを計算できる。従って、記録再生装置がコンテンツの利用毎に必要となっていたKRB復号処理等の計算量を減少させることが可能となる。

請求の範囲

1. 暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理装置内の記憶領域に格納する

ことを特徴とする情報処理装置。

2. 前記情報処理装置固有のキーは、前記各情報処理装置固有のリーフキーであることを特徴とする請求の範囲第1項記載の情報処理装置。

3. 前記キーブロックは、前記記憶手段に記憶されたノードキーを更新するための更新ノードキーと前記復号用キーを含んでおり、

前記更新ノードキーは、下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーによって暗号化されており、

前記復号用キーは、前記更新ノードキーで暗号化されており、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて前記更新ノードキーを復号して前記更新ノードキーを取得すると共に、前記取得した更新ノードキーを用いて前記復号用キーを算出する

ことを特徴とする請求の範囲第1項記載の情報処理装置。

4. 前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて格納することを特徴とする請求の範囲第1項記載の情報処理装置。

5. 前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記情報処理装置固有の識別情報と対応付けて格納することを特徴とする請求の範囲第1項記載の情報処理装置。

6. 前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーで復号される暗号化されたデータの識別情報と対応付けて格納することを特徴とする請求の範囲第1項記載の情報処理装置。

7. 前記復号用キーは、前記暗号化されたデータを復号するためのコンテンツキーであることを特徴とする請求の範囲第1項記載の情報処理装置。

8. 前記復号用キーは、前記記録媒体に割り当てられたキーであり、暗号化されたデータを復号するために用いられるメディアキーであることを特徴とする請求の範囲第1項記載の情報処理装置。

9. 前記復号用キーは、他の情報処理装置と共通に保持されるキーであり、前記暗号化されたデータを復号するために用いられるマスターキーであることを特徴とする請求の範囲第1項記載の情報処理装置。

10. 暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納する

ことを特徴とする情報処理装置。

11. 暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、

暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納することを特徴とする情報処理装置。

12. 暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、復号処理を実行する復号処理手段を有し、

前記復号処理手段は、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、

復号用キーが検出されなかった場合には、前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する

ことを特徴とする情報処理装置。

13. 前記復号処理手段は、復号用キーが検出されなかった場合には、前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて算出した前記復号用キーに対して前記情報処理装置固有のキーを用いた暗号化処理を行い、前記記録媒体又は前記情報処理装置内の記憶領域に格納することを特徴

とする請求の範囲第12項記載の情報処理装置。

14. 前記復号処理手段は、復号用キーが検出された場合には、前記各情報処理装置固有のキーを用いて暗号化された復号用キーを復号することを特徴とする請求の範囲第12項記載の情報処理装置。

15. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行い、

暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納する

ことを特徴とする情報処理方法。

16. 前記情報処理装置固有のキーは、前記各情報処理装置固有のリーフキーであることを特徴とする請求の範囲第15項記載の情報処理方法。

17. 前記キーブロックは、前記情報処理装置に保有されたノードキーを更新するための更新ノードキーと前記復号用キーを含んでおり、

前記更新ノードキーは、下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーによって暗号化されており、

前記復号用キーは、前記更新ノードキーで暗号化されており、

前記キーブロックの復号処理は、前記情報処理装置に保有された前記ノードキー又はリーフキーの少なくともいずれかを用いて前記更新ノードキーを復号して前記更新ノードキー取得する処理であり、

前記復号用キーの算出処理は、前記取得した更新ノードキーを用いて前記復号用キーを算出する処理である

ことを特徴とする請求の範囲第15項記載の情報処理方法。

18. 前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて格納することを特徴とする請求の範囲第15項記載の情報処理方法。

19. 前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記情報処理装置固有の識別情報と対応付けて格納することを特徴とする請求の範囲第15項記載の情報処理方法。

20. 前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーで復号される暗号化されたデータの識別情報と対応付けて格納することを特徴とする請求の範囲第15項記載の情報処理方法。

21. 前記復号用キーは、前記暗号化されたデータを復号するためのコンテンツキーであることを特徴とする請求の範囲第15項記載の情報処理方法。

22. 前記復号用キーは、前記記録媒体に割り当てられたキーであり、暗号化されたデータを復号するために用いられるメディアキーであることを特徴とする請求の範囲第15項記載の情報処理方法。

23. 前記復号用キーは、他の情報処理装置と共通に保持されるキーであり、前記暗号化されたデータを復号するために用いられるマスターキーであることを特徴とする請求の範囲第15項記載の情報処理方法。

24. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納することを特徴とする情報処理方法。

25. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納することを特徴とする情報処理方法。

26. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、

前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、

復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキープロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出することを特徴とする情報処理方法。

27. 復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて算出した前記復号用キーに対して前記情報処理方法固有のキーを用いた暗号化処理を行い、前記記録媒体又は前記情報処理装置内の記憶領域に格納することを特徴とする請求

の範囲第26項記載の情報処理方法。

28. 復号用キーが検出された場合には、前記各情報処理装置固有のキーを用いて暗号化された復号用キーを復号することを特徴とする請求の範囲第26項記載の情報処理方法。

29. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行うステップと、

暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

30. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

31. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノ

ードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

32. 複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において実行されるコンピュータ・プログラムであって、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込むステップと、

前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索するステップと、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップと、

復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップとを具備することを特徴とするコンピュータ・プログラム。

33. 記録された情報が情報処理装置によって読み出し可能なように構成された情報記録媒体であって、

前記情報処理装置に固有のキーによって暗号化処理を施した、暗号化されたデータを復号するための復号用キーが、前記情報処理装置の識別情報と関連付けてキー格納テーブルとして記録されていることを特徴とする情報記録媒体。

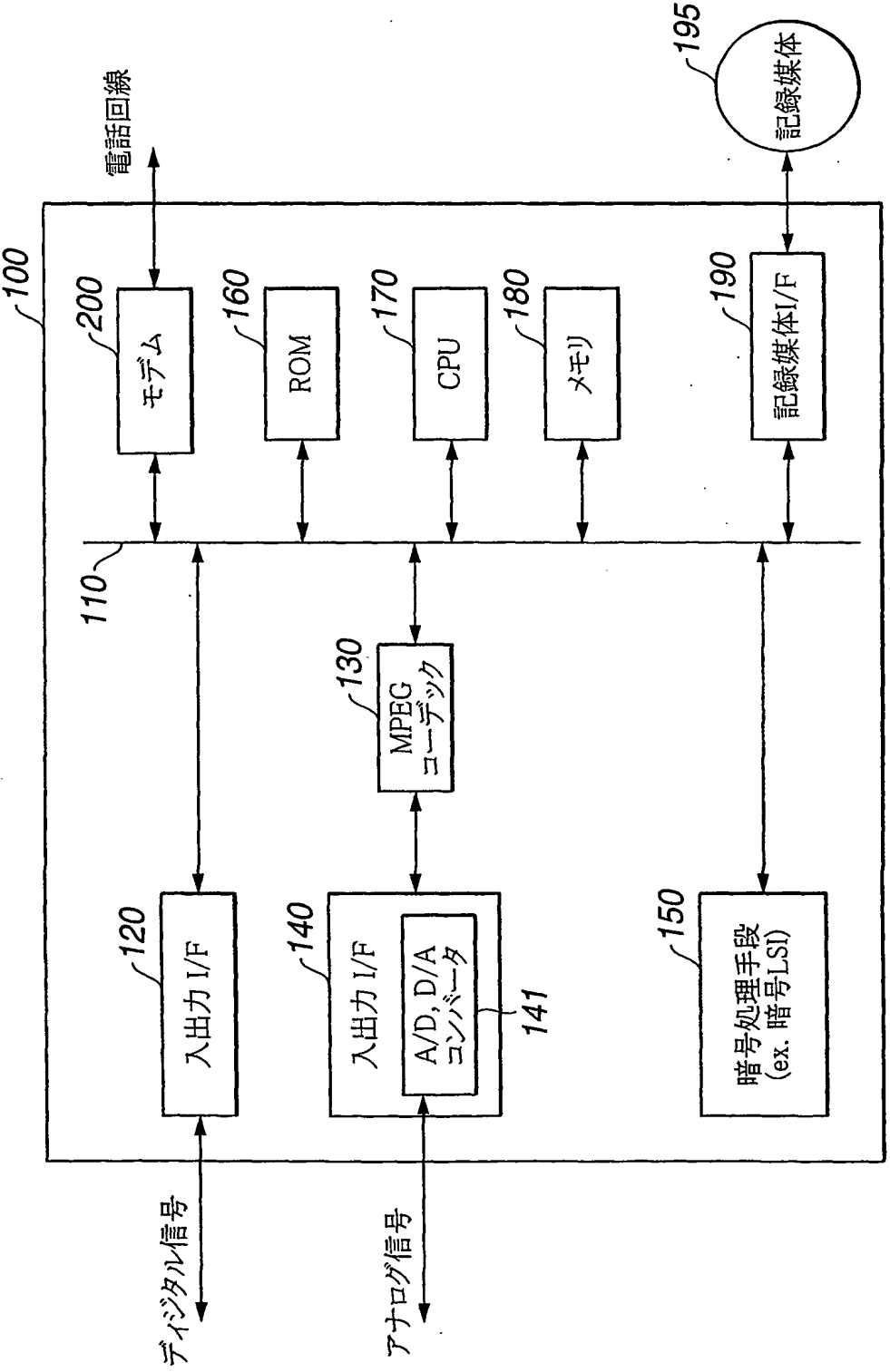


FIG.1

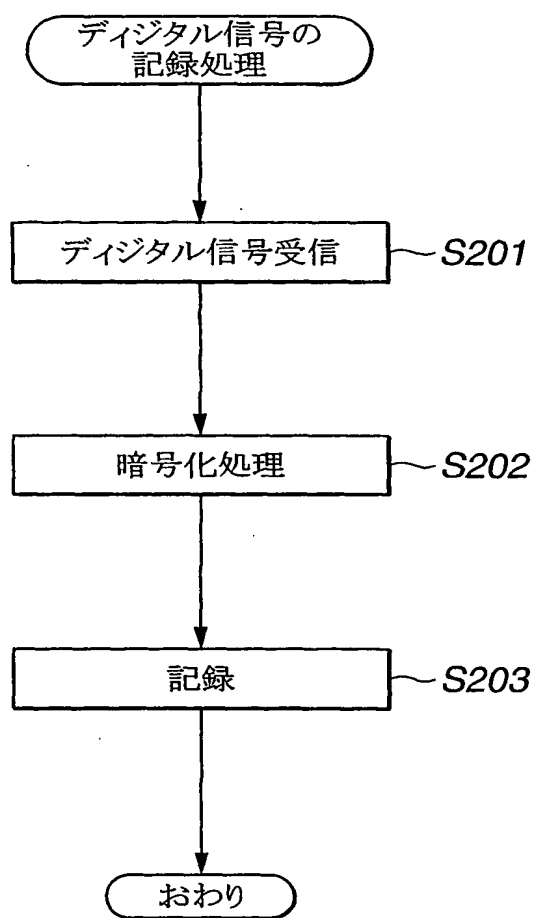


FIG.2A

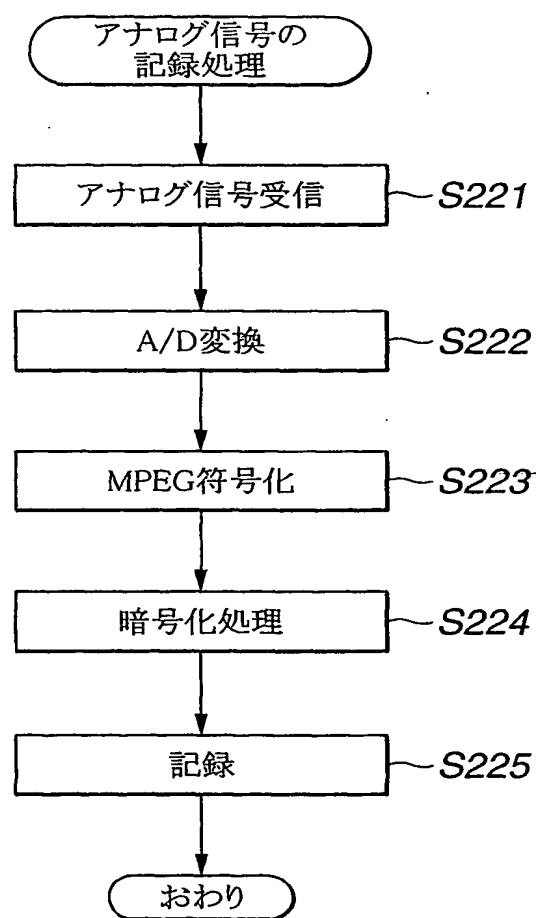


FIG.2B

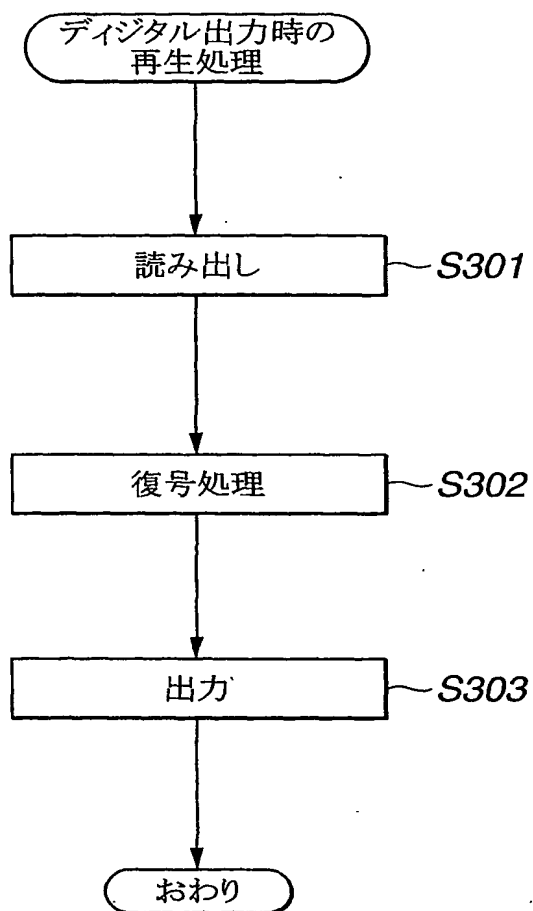


FIG.3A

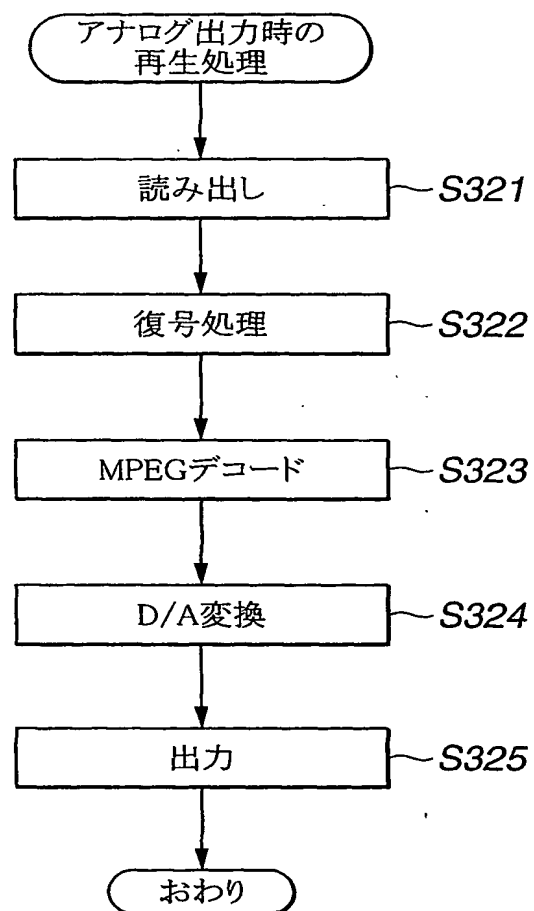


FIG.3B

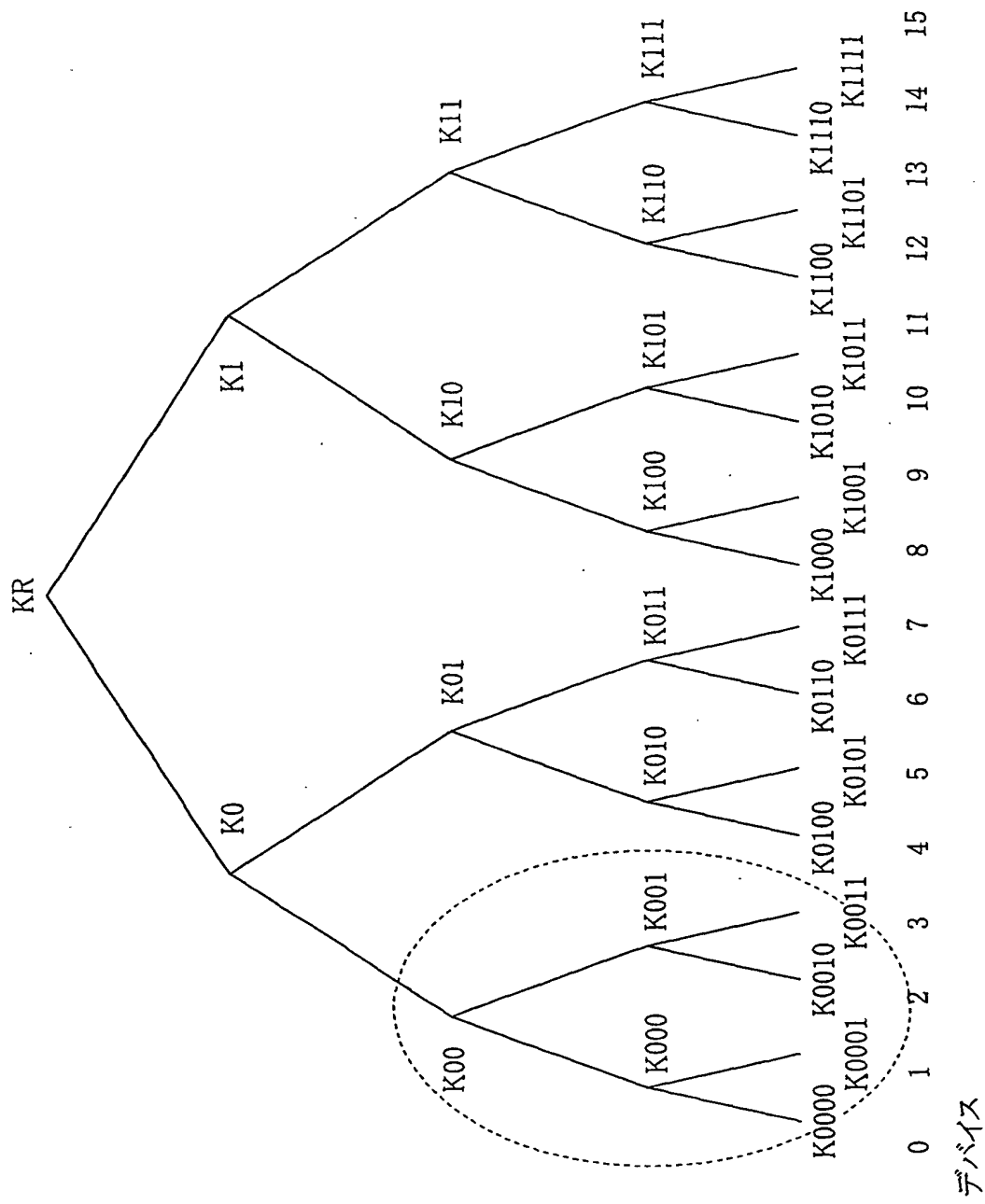


FIG.4

5/29

キー更新ブロック (KRB : Key Renewal Block) 例1
デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代 (Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5A

キー更新ブロック (KRB : Key Renewal Block) 例2
デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代 (Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5B

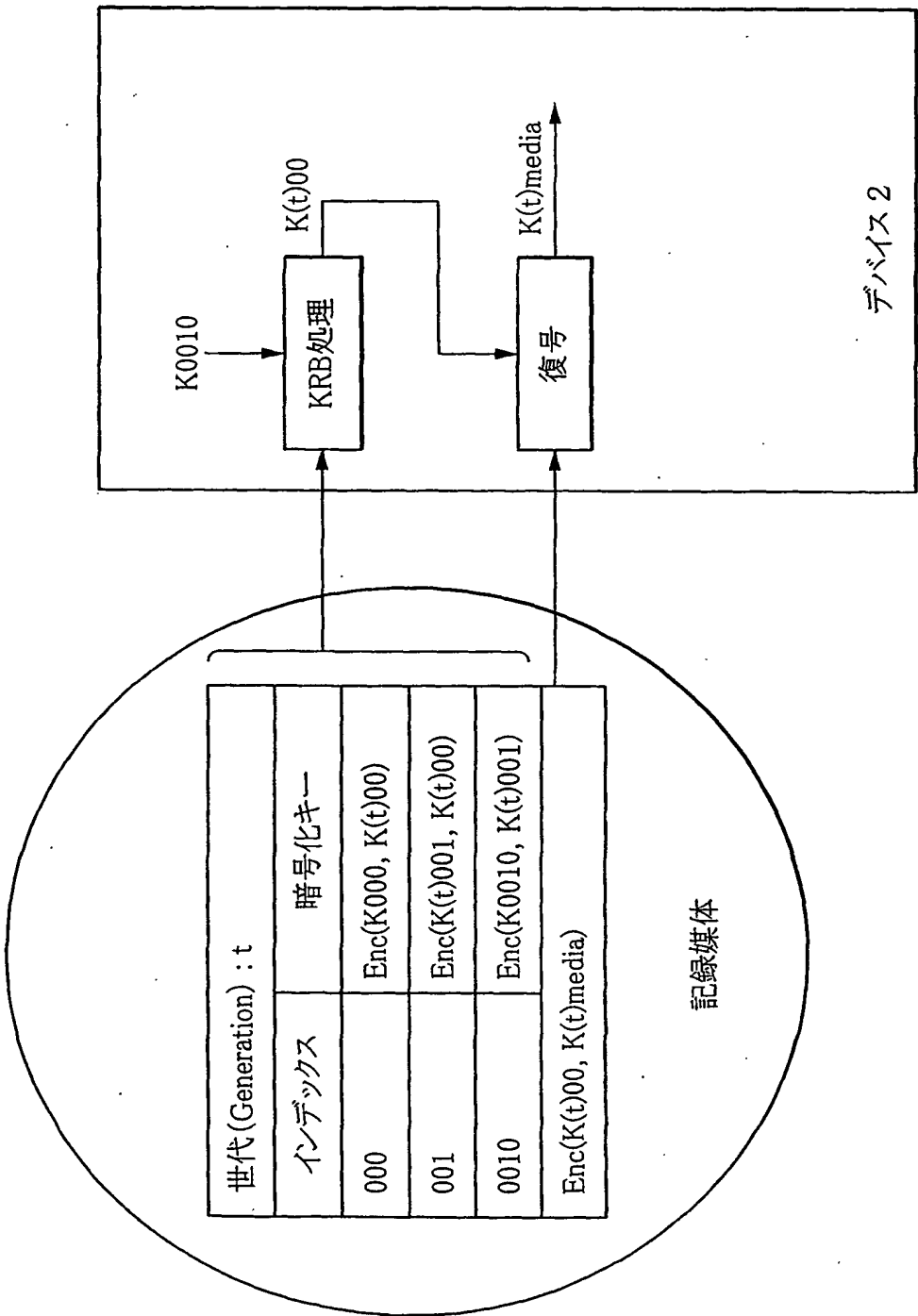


FIG.6

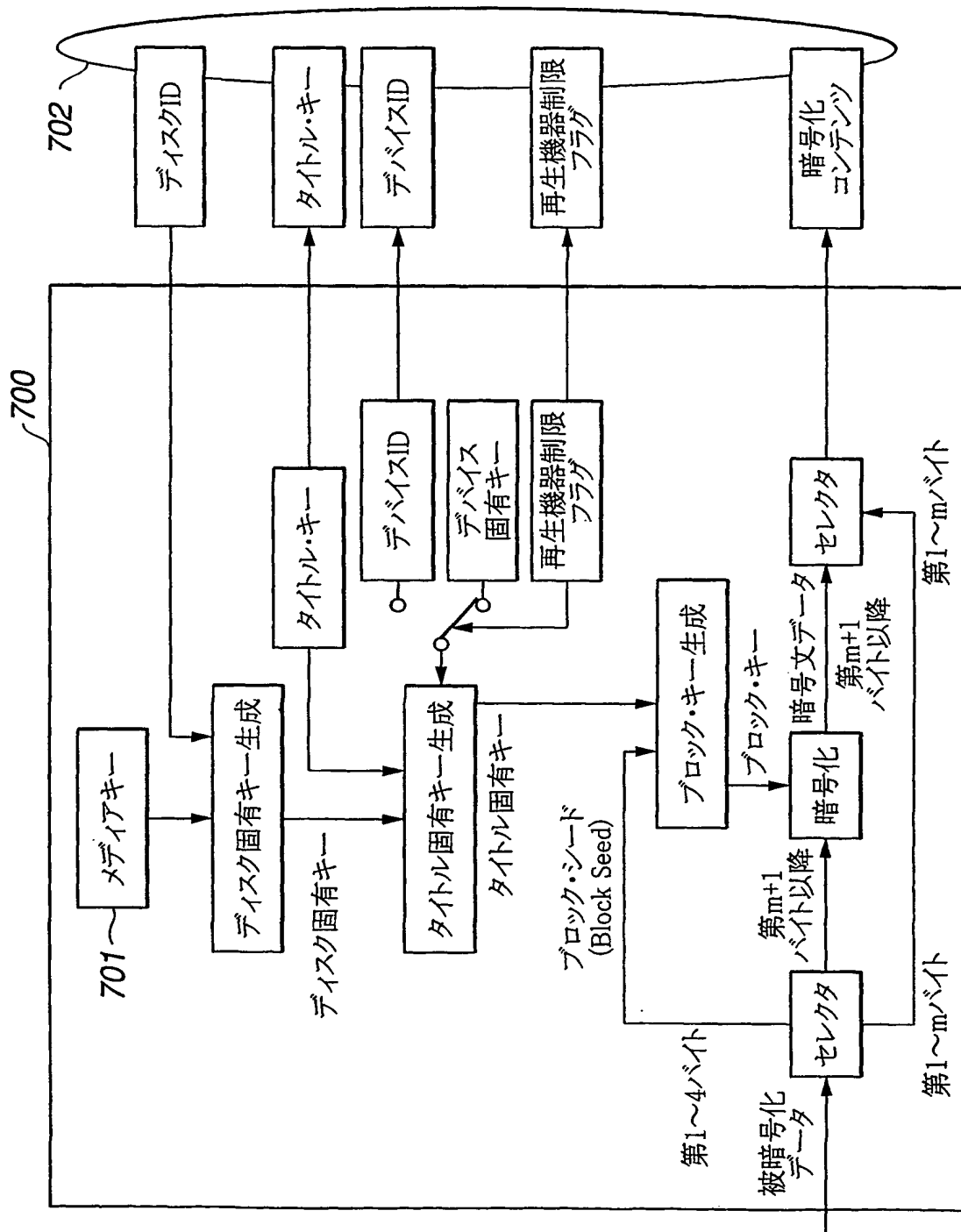


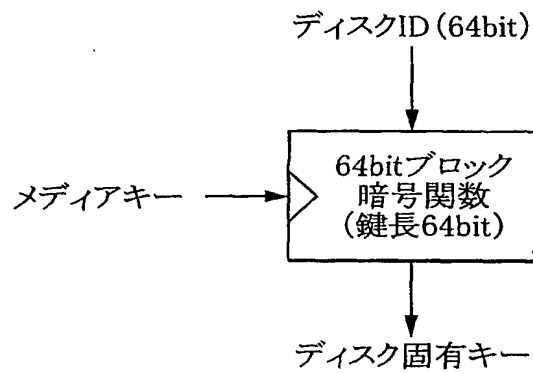
FIG.7

8/29

例1

ディスク固有キー生成例

入力
メディアキー (64bit)
ディスクID (64bit)



出力
ディスク固有キー (64bit)

例2

メディアキー||ディスクID

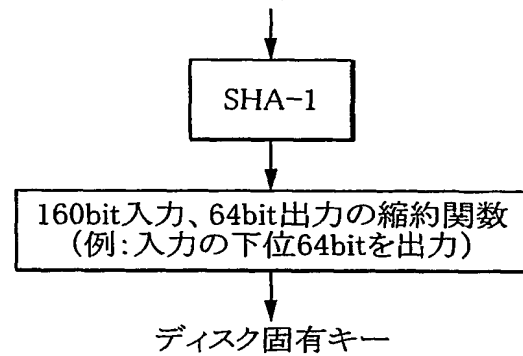
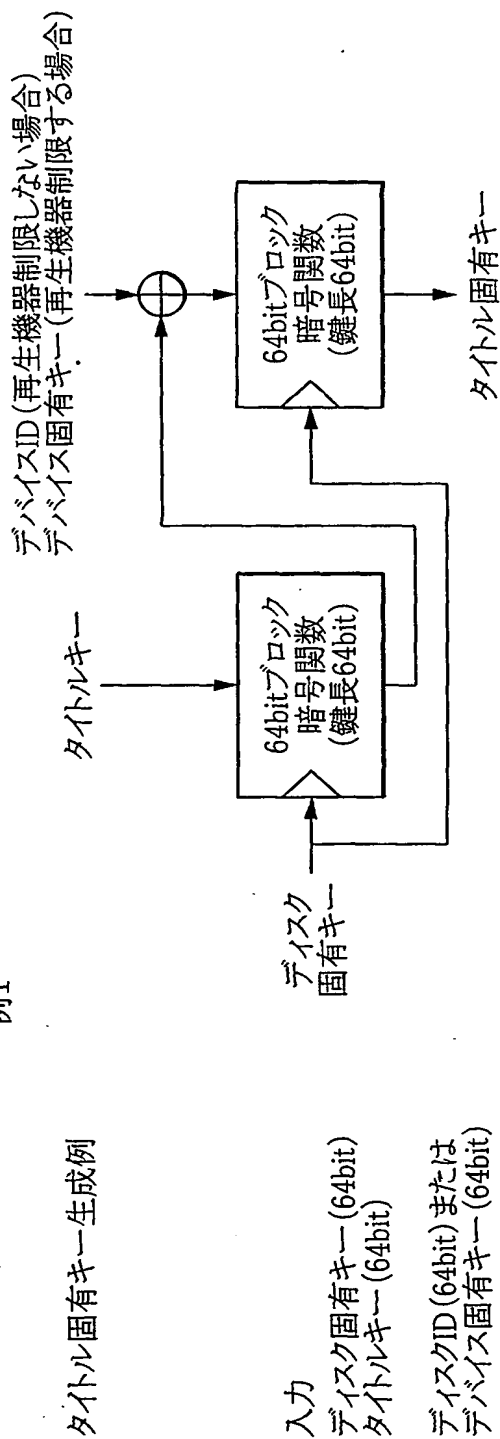


FIG.8

9/29

例1

タイトル固有キー生成例



入力
ディスク固有キー (64bit)
タイトル固有キー (64bit)
ディスクID (64bit) または
デバイス固有キー (64bit)

出力

タイトル固有キー (64bit)

例2

ディスク固有キー || タイトルキー || デバイスID (再生機器制限しない場合)
ディスク固有キー || タイトルキー || デバイス固有キー (再生機器制限する場合)

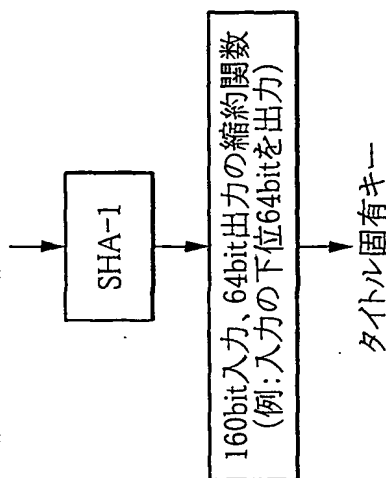


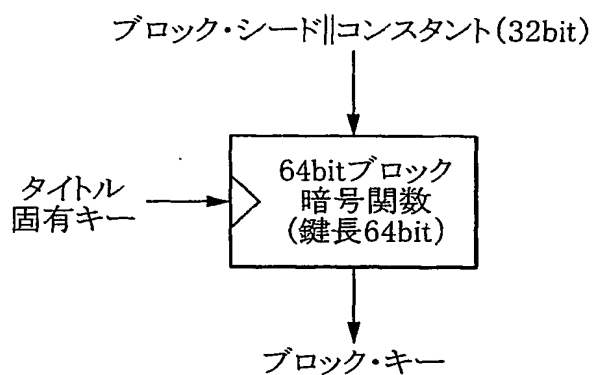
FIG.9

10/29

例1

ブロック・キー生成例

入力
ブロック・シード (32bit)
タイトル固有キー (64bit)



出力
ブロック・キー (64bit)

例2

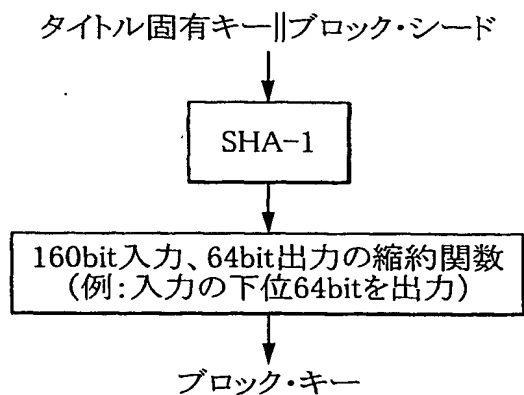


FIG.10

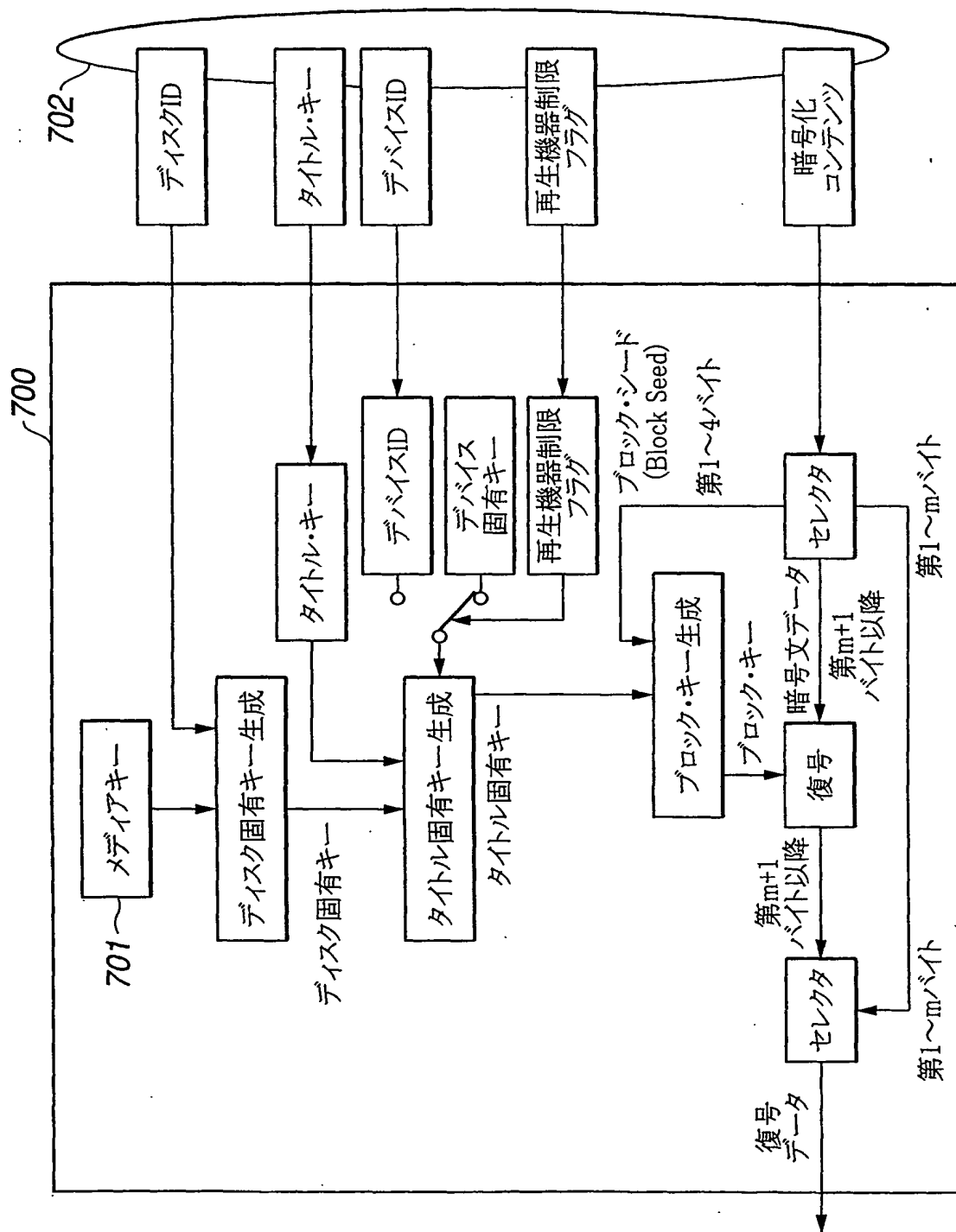


FIG.11

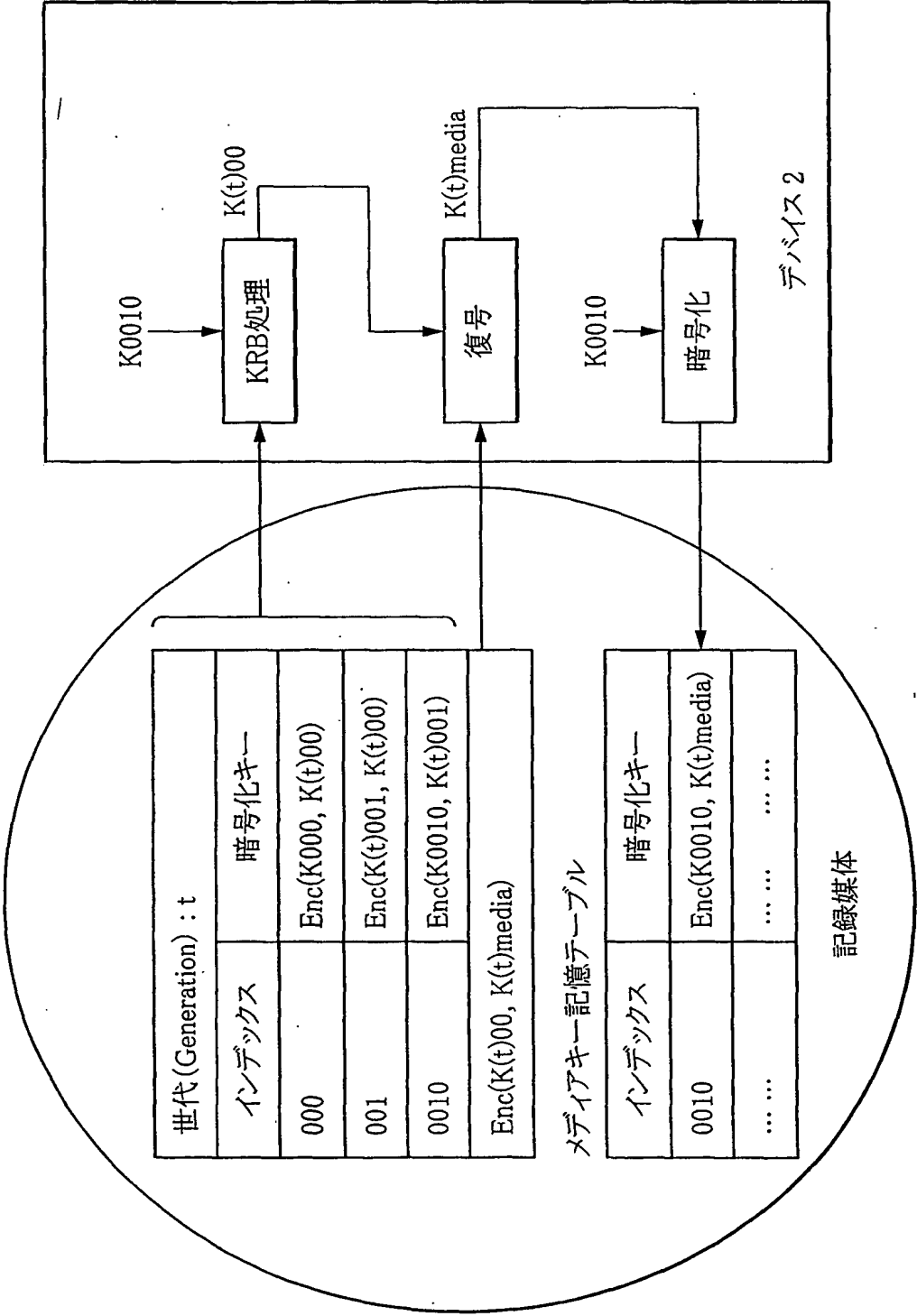


FIG.12

13/29

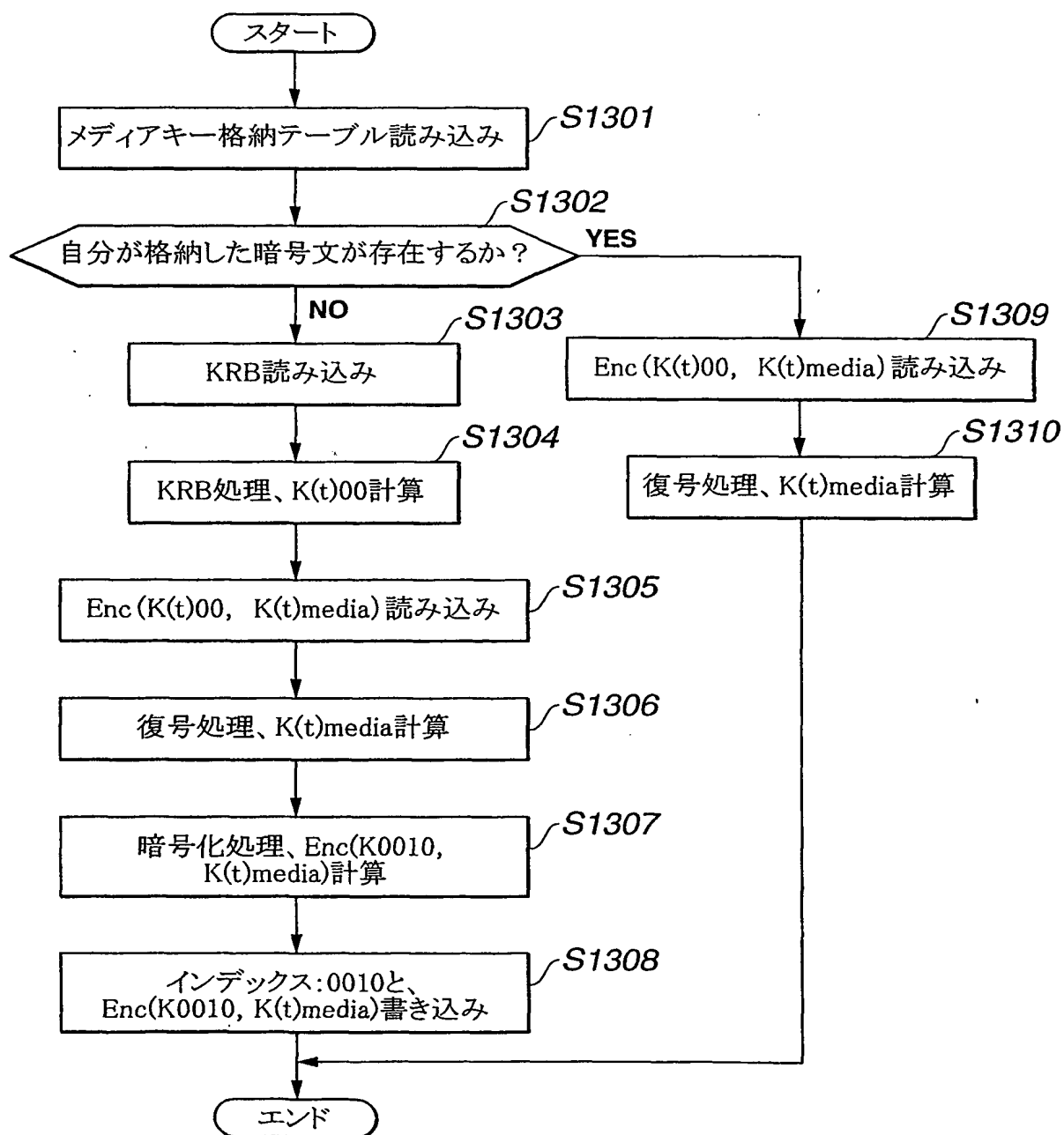


FIG.13

14/29

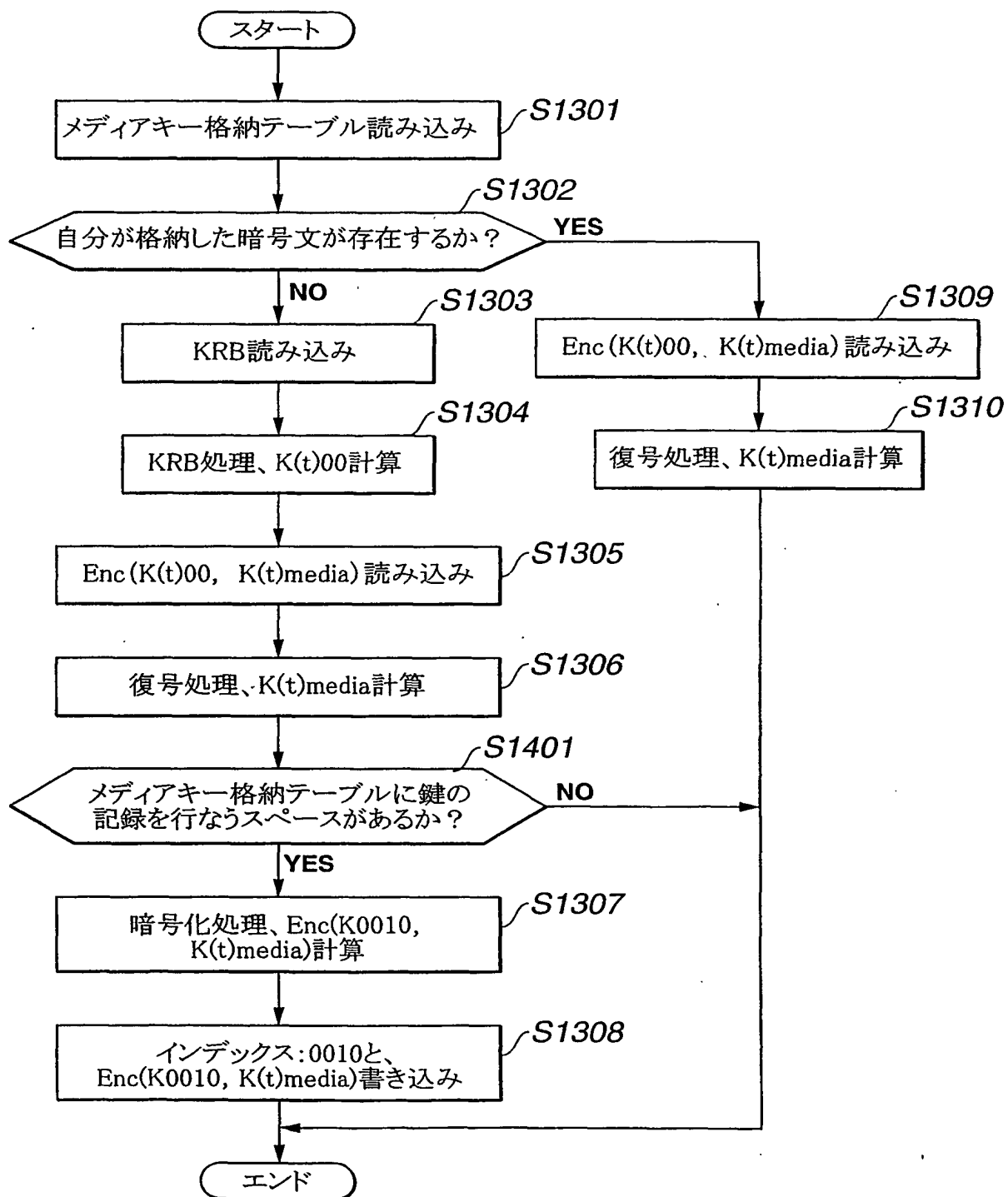


FIG.14

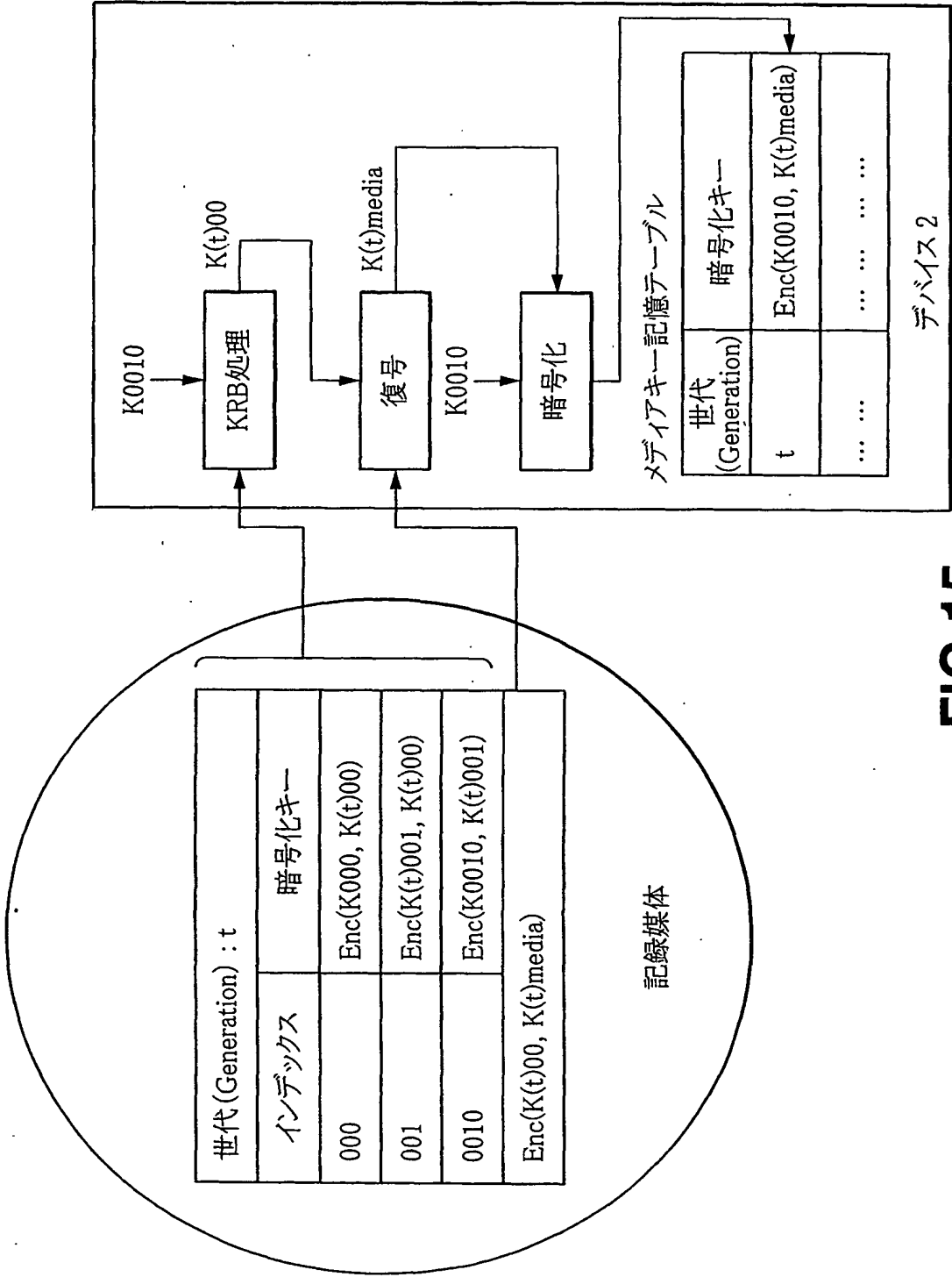


FIG.15

16/29

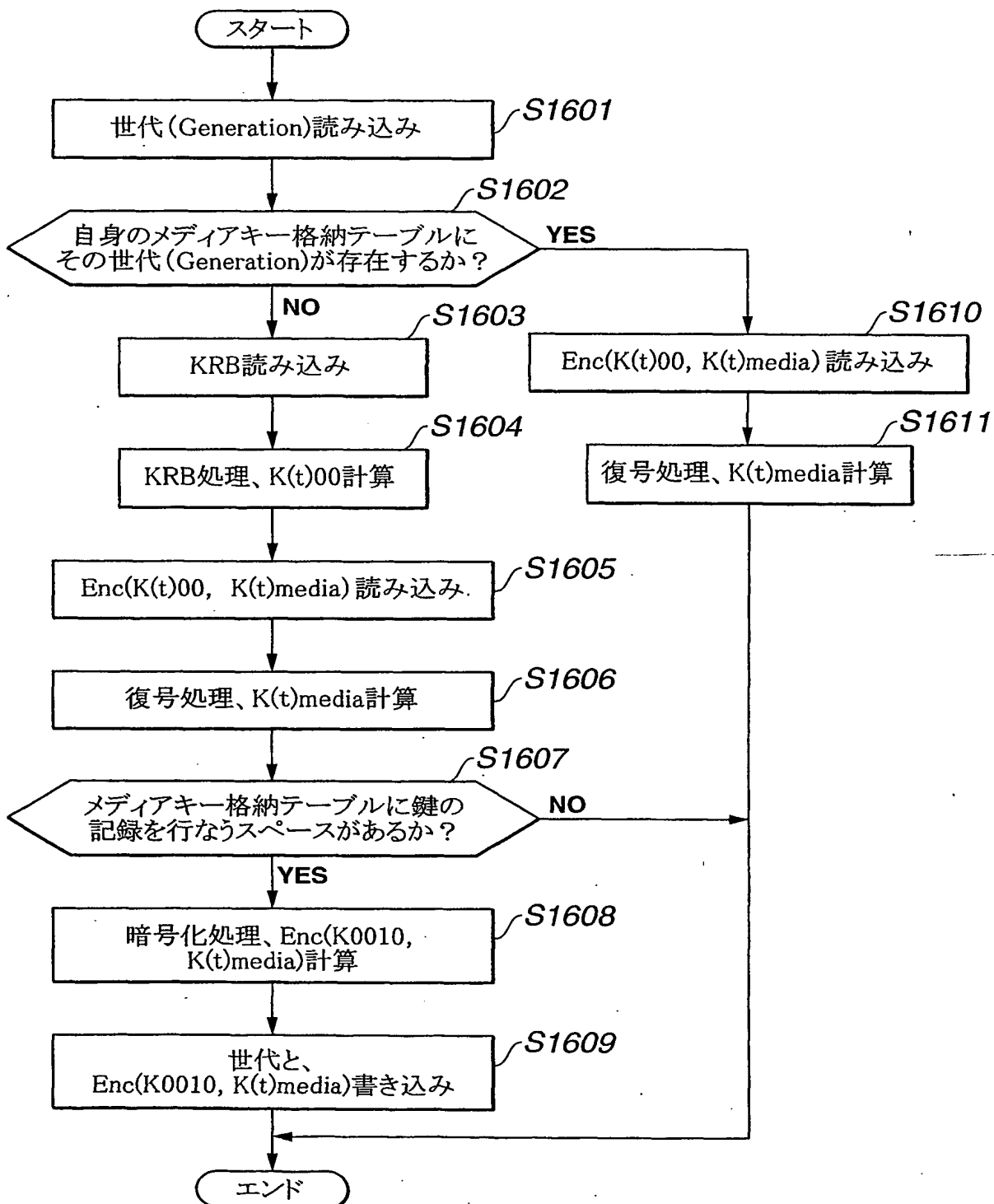


FIG.16

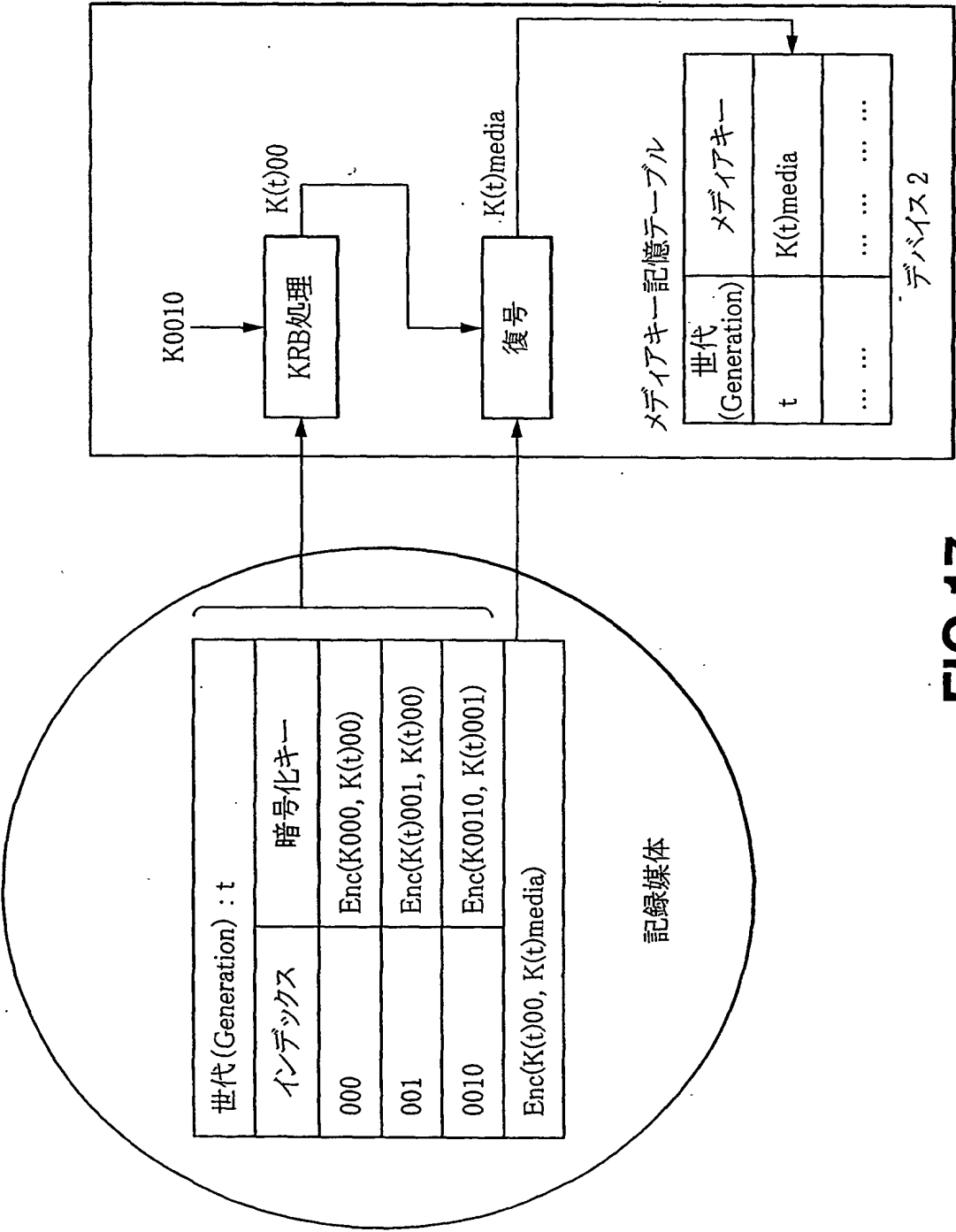


FIG.17

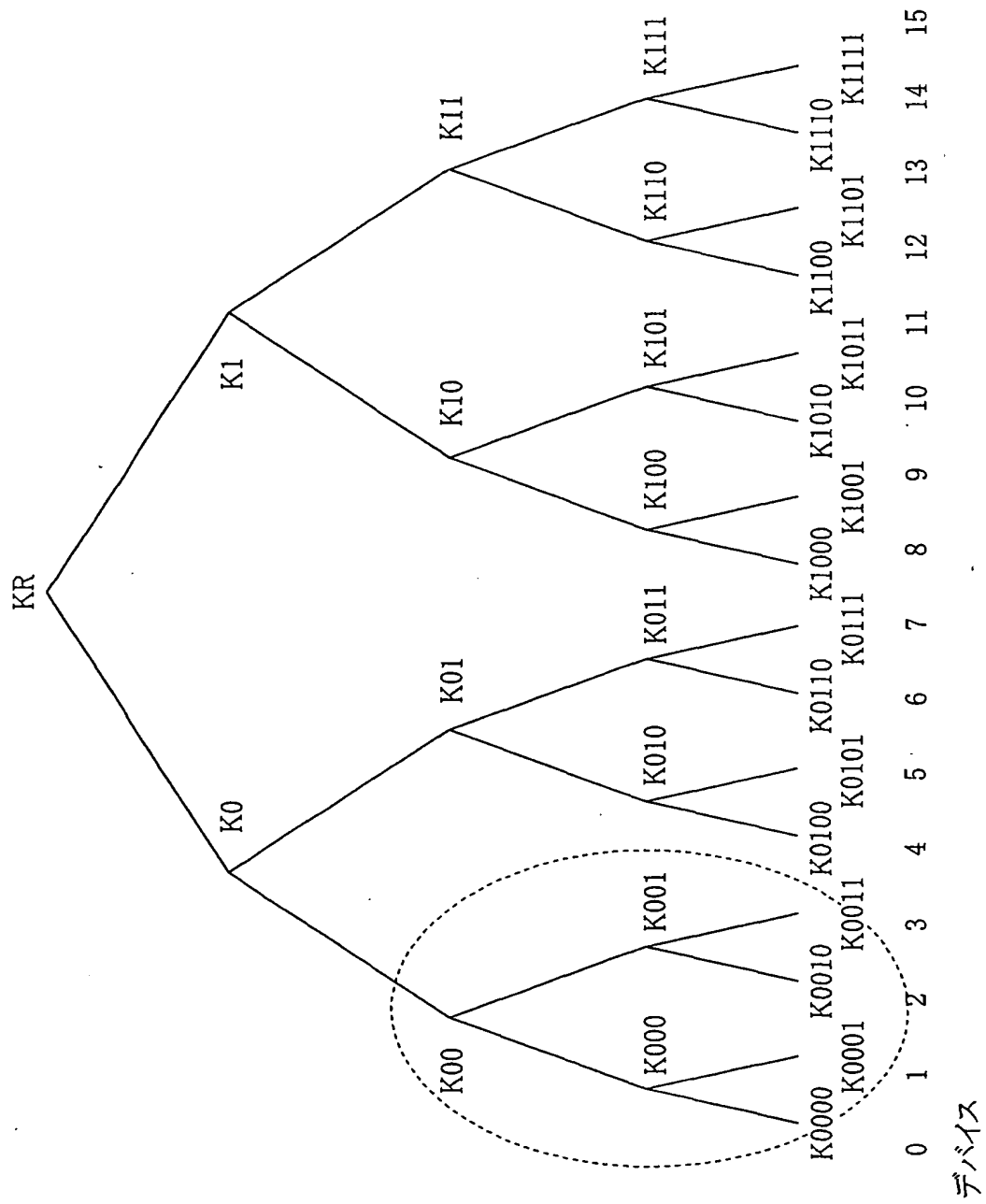


FIG.18

19/29

キー更新ブロック(KRB : Key Renewal Block) 例1
 デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
0	$Enc(K(t)0, K(t)R)$
00	$Enc(K(t)00, K(t)0)$
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

FIG.19A

キー更新ブロック(KRB : Key Renewal Block) 例2
 デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

FIG.19B

コンテンツID : s	
インデックス	暗号化キー
0	$\text{Enc}(K(t)0, K(t)R)$
.00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$
$\text{Enc}(K(t)R, K(s)\text{content})$	
$\text{Enc}(K(s)\text{content}, \text{content})$	

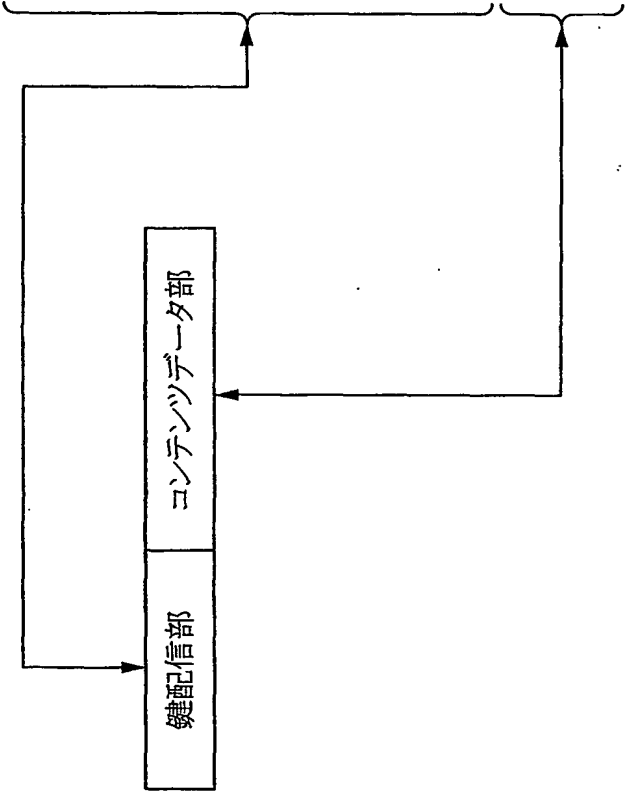


FIG.20

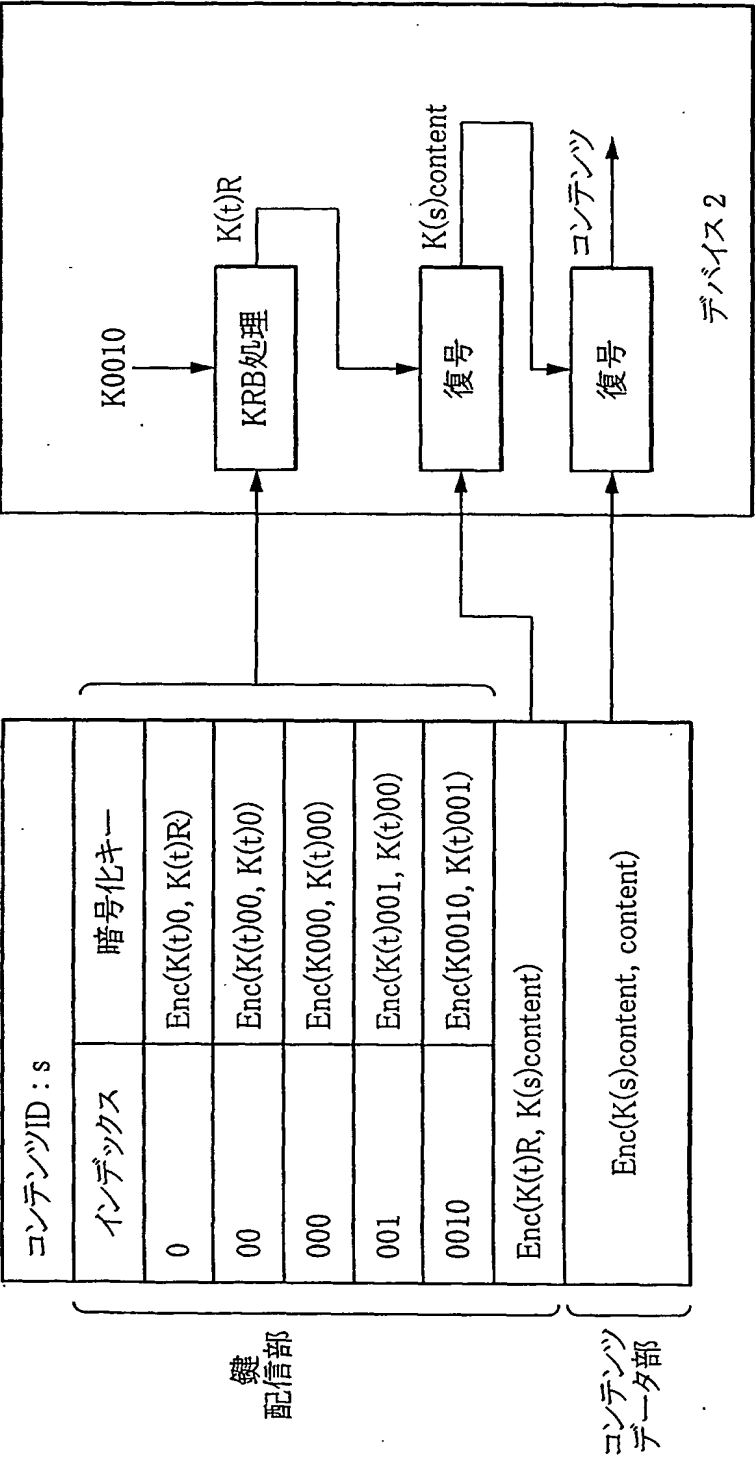


FIG.21

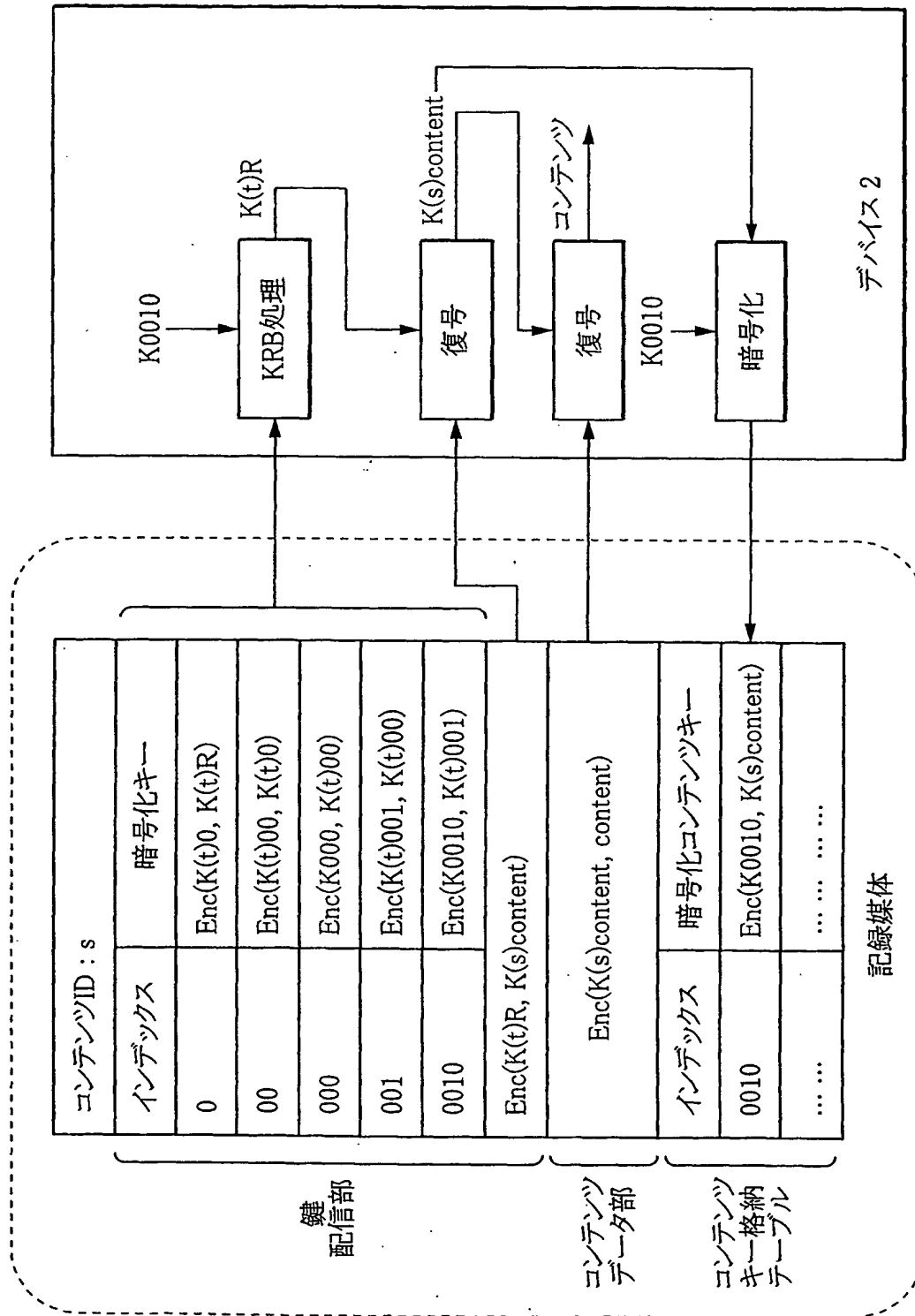


FIG.22

23/29

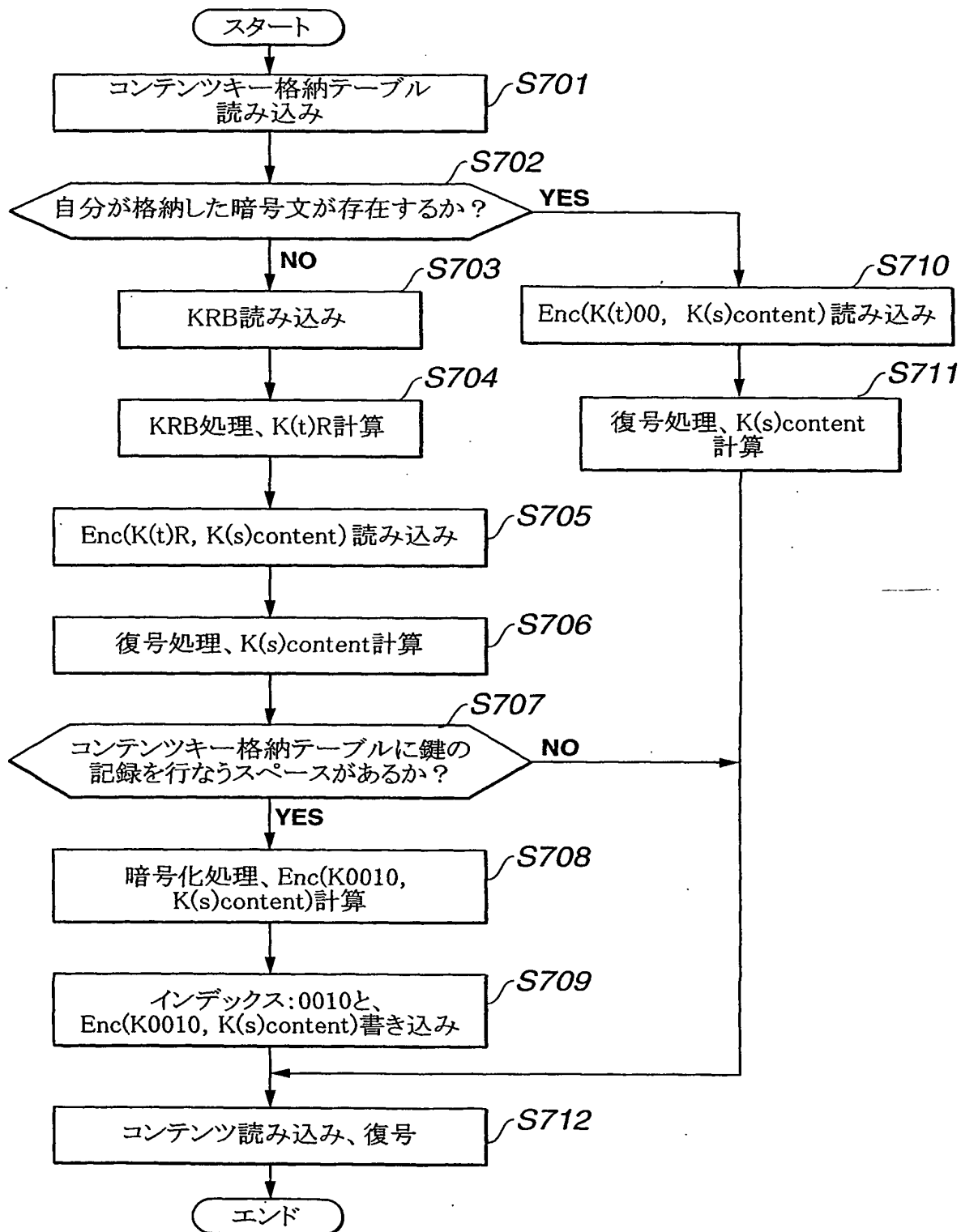


FIG.23

24/29

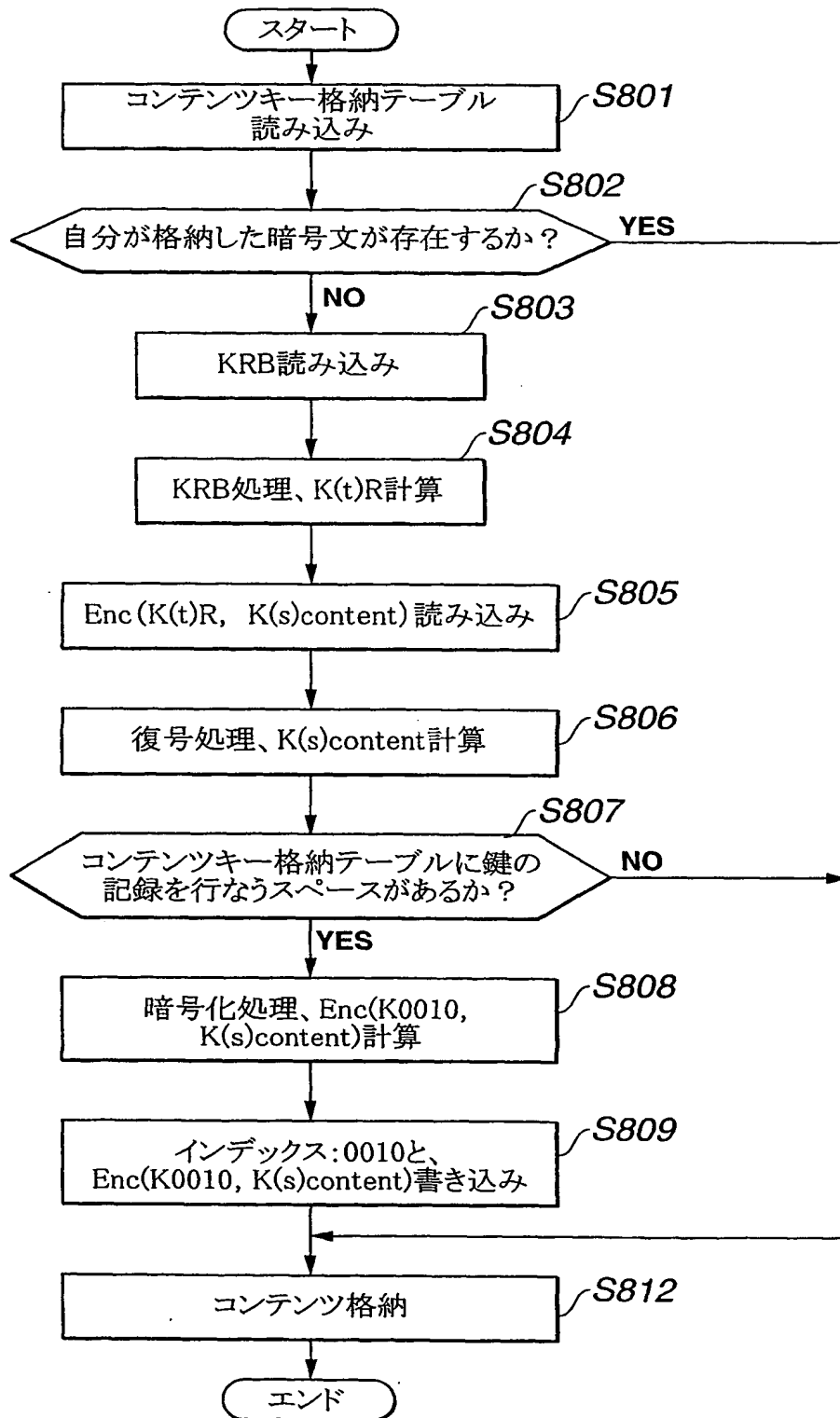


FIG.24

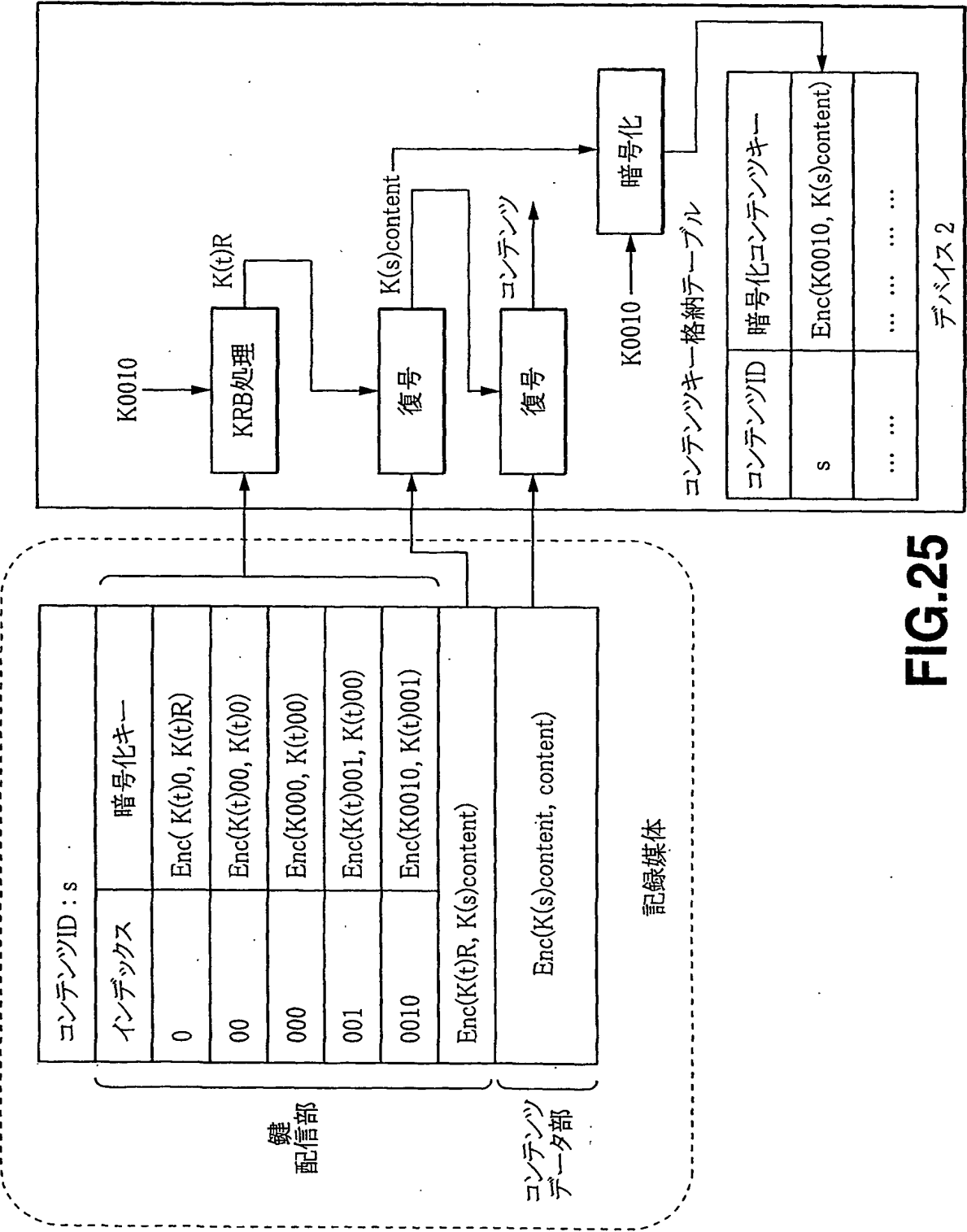


FIG.25

26/29

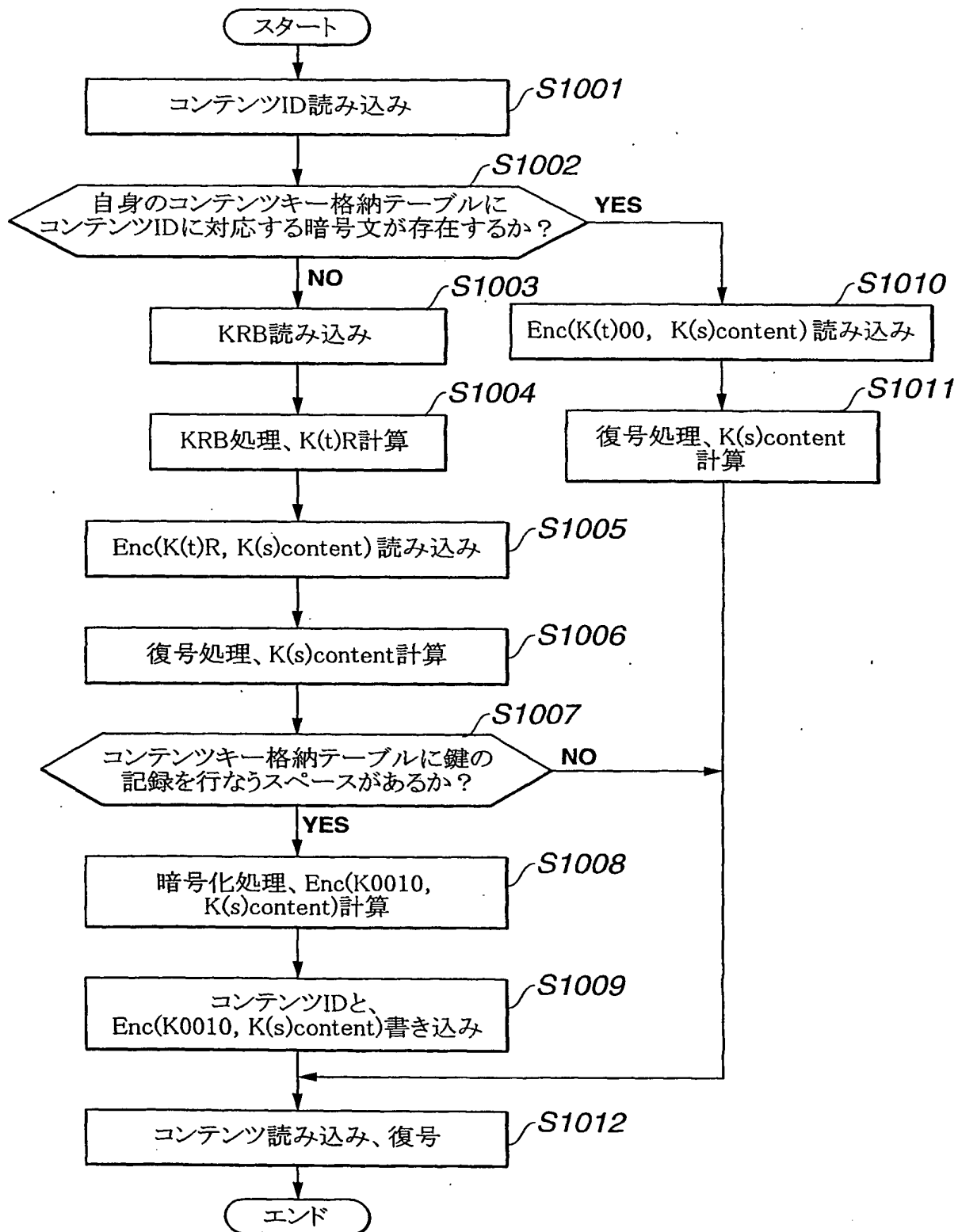


FIG.26

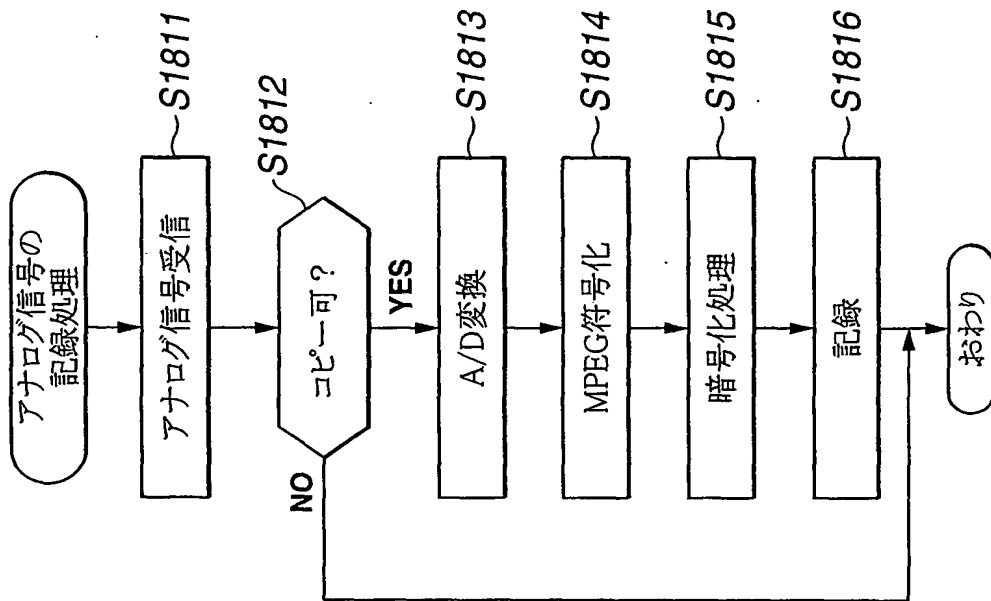


FIG. 27B

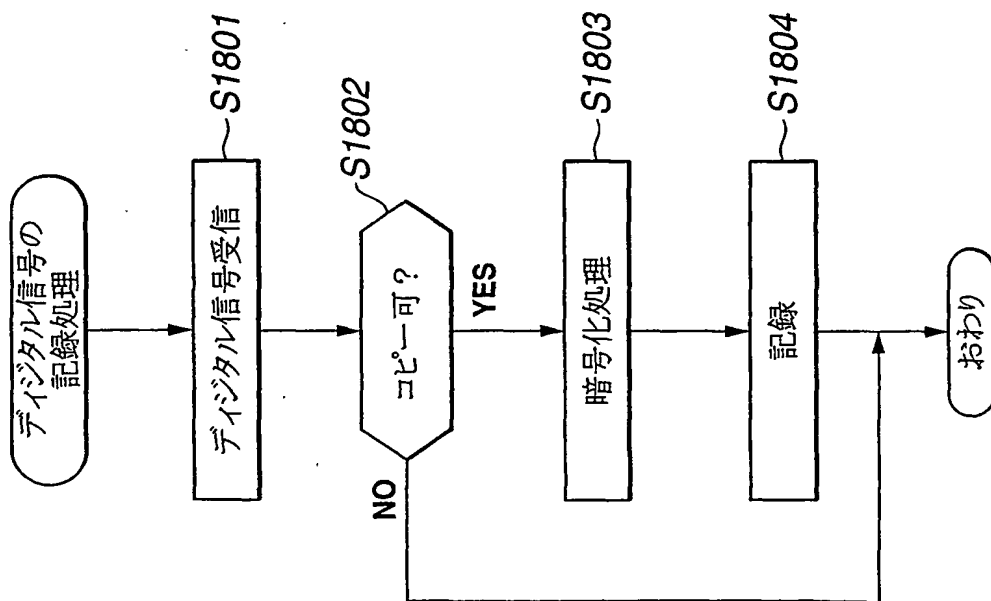


FIG. 27A

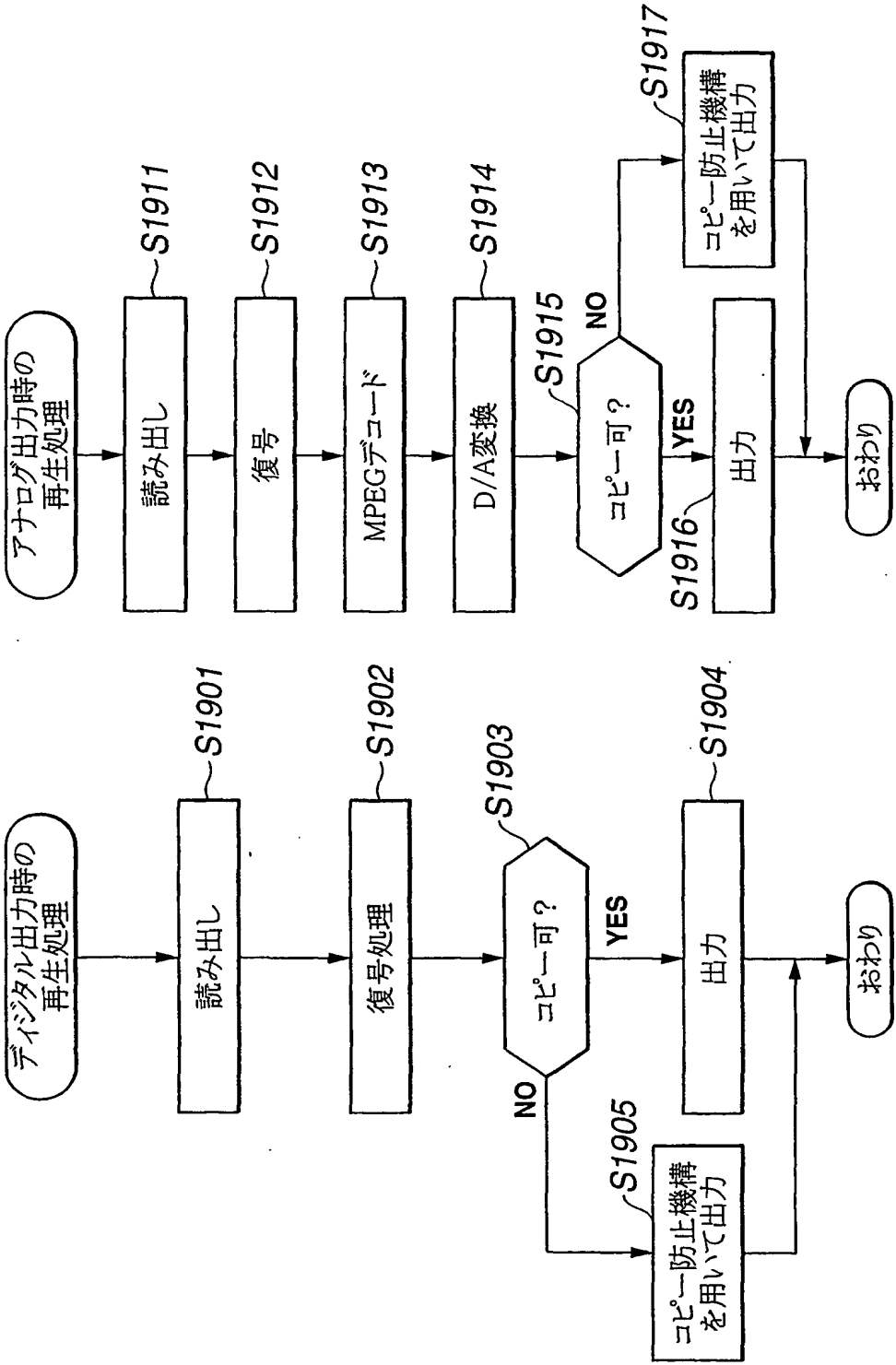


FIG. 28A

FIG. 28B

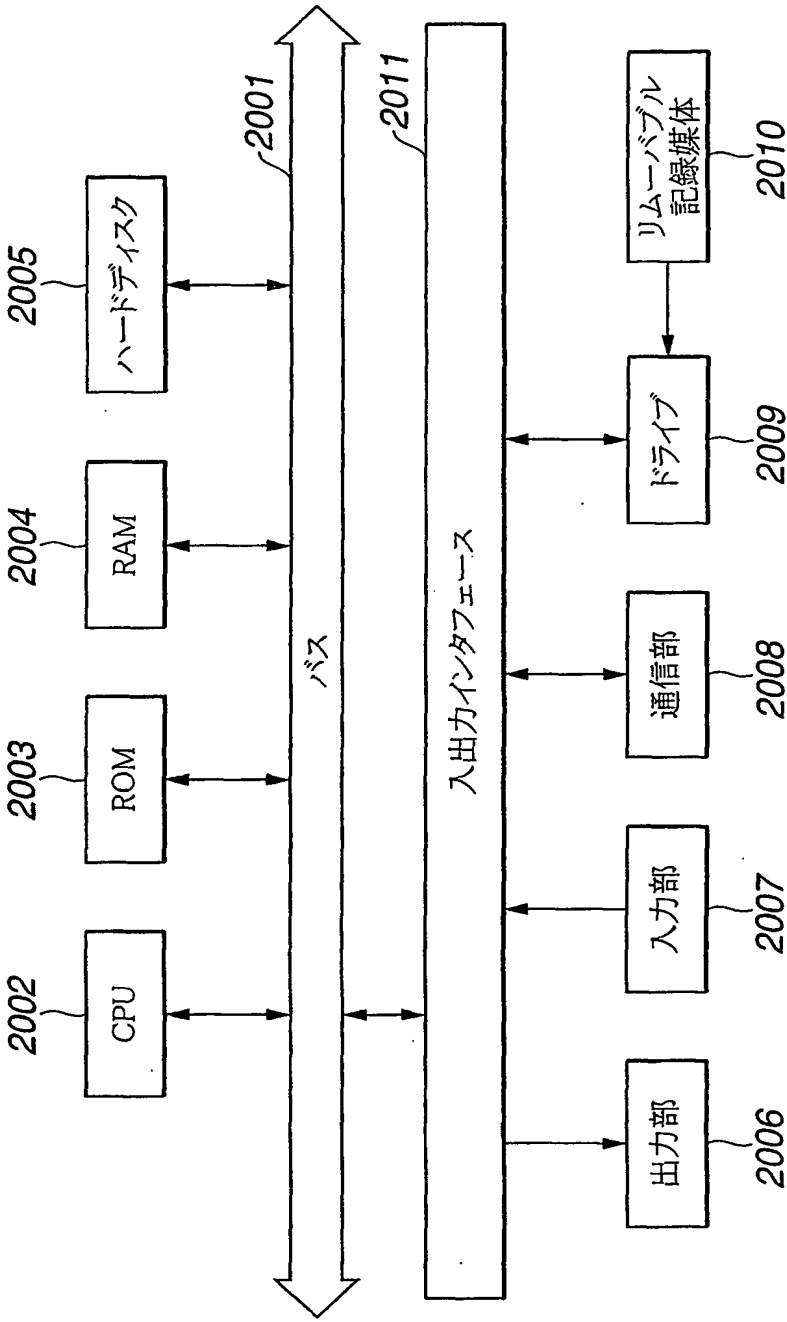


FIG.29

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST科学技術文献データベース key, tree, generation, DVD

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WALDVOGEL, M. et al.	10, 24, 30
Y	The VersaKey Framework: Versatile Group Key Management. IEEE Journal on Selected Areas in Communications. September 1999, Vol. 17, No. 9, p. 1614-1631, especially pp. 1616-1621	1- 9, 11, 15- 23, 25, 29, 31
A		12-14, 26-28, 32
Y	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワ ークの安全性, 日本経済新聞社, 29.7月. 1983 (29.07.83), p. 201-206 (特にp. 204 3 データ暗号鍵の登録 を参照)	1- 9, 15-23, 29

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

07.09.01

国際調査報告の発送日

18.09.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M

9.3.6.4

電話番号 03-3581-1101 内線 3597

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	EP 969667 A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 5.1月.2000(05.01.00), 第33-39段落 & JP 2000-23137 A, 第61, 66, 67段落 & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11, 25, 31
Y	JP 9-115241 A (ソニー株式会社) 2.5月.1997(02.05.97), 第21, 22, 28段落 & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (ソニー株式会社) 30.11月.1999(30.11.99), 第16, 18, 19, 57, 58段落 & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9.7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	1-32
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98, 1998, p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-33

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の5群の発明に区分される。

1. 請求の範囲1-9, 15-23, 29
2. 請求の範囲10, 24, 30
3. 請求の範囲11, 25, 31
4. 請求の範囲12-14, 26-28, 32
5. 請求の範囲33

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05327

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001

Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST FILE on Science and Technology key, tree, generation, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WALDVOGEL, M. et al., "The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, September, 1999, Vol.17, No.9, pages 1614 to 1631, especially pages 1616 to 1621	10, 24, 30
Y		1-9, 11, 15-23, 25, 29, 31
A		12-14, 26-28, 32
Y	supervised by Shin ICHIMATSU, "Data Hogo to Angou-ka no Kenkyu; Computer Network no Anzensei", Nippon Keizai Shinbunsha, 29 July, 1983 (29.07.83), pages 201 to 206, (especially, page 204, 3 Data Angou Kagi no Touroku)	1-9, 15-23, 29
Y	EP 969667 A2 (Matsushita Electric Industrial Co., Ltd.), 05 January, 2000 (05.01.00), Par. Nos. [0033] to [0039] & JP 2000-23137 A Par. Nos. [0061], [0066], [0067] & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11, 25, 31

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
07 September, 2001 (07.09.01)

Date of mailing of the international search report
18 September, 2001 (18.09.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05327

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-115241 A (Sony Corporation), 02 May, 1997 (02.05.97), Par. Nos. [0021], [0022], [0028] & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (Sony Corporation), 30 November, 1999 (30.11.99), Par. Nos. [0016], [0018], [0019], [0057], [0058] & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (IBM Japan, Ltd.), 09 July, 1999 (09.07.99), Par. Nos. [0009] to [0011], [0017] to [0022] & CN 1224962 A	1-32
A	WONG, C. K. et al., "Secure Group Communications Using Key Graphs", In: Proceedings of ACM SIGCOMM'98, (1998), pages 68 to 79, especially, 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
PA	Makoto TATEBAYASHI et al., "Kiroku Media no Contents Hogo System", 2000 nen Denshi Joho Tsuushin Gakkai Kiso Kyoukai Society Taikai Kouen Ronbunshuu, 07 September, 2000 (07.09.00), pages 367 to 368	1-33

INTERNATIONAL SEARCH REPORT

In International application No.
PCT/JP01/05327

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This applied invention is classified into the following five groups of inventions:

1. Claims 1-9, 15-23, 29,
2. Claims 10, 24, 30,
3. Claims 11, 25, 31,
4. Claims 12-14, 26-28, 32, and
5. Claim 33.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

E P . U S P C T

国際調査報告

(法 8 条、法施行規則第40、41条)
(PCT 18条、PCT規則43、44)

出願人又は代理人 の書類記号 SK 01 PCT 87	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JPO1/05327	国際出願日 (日.月.年) 21.06.01	優先日 (日.月.年) 21.06.00
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT 18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☒ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 12 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の5群の発明に区分される。

1. 請求の範囲1-9, 15-23, 29
2. 請求の範囲10, 24, 30
3. 請求の範囲11, 25, 31
4. 請求の範囲12-14, 26-28, 32
5. 請求の範囲33

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G10K15/02, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST 科学技術文献データベース key, tree, generation, DVD

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WALDVOGEL, M. et al. The VersaKey Framework: Versatile Group Key Management.	10, 24, 30
Y	IEEE Journal on Selected Areas in Communications. September 1999, Vol. 17, No. 9, p. 1614-1631, especially pp. 1616-1621	1- 9, 11, 15- 23, 25, 29, 31
A		12-14, 26-28, 32
Y	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワ ークの安全性, 日本経済新聞社, 29. 7月. 1983 (29. 07. 83), p. 201-206 (特に p. 204 3 データ暗号鍵の登録 を参照)	1- 9, 15-23, 29

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

07. 09. 01

国際調査報告の発送日

18.09.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M

9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	EP 969667 A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 5.1月.2000(05.01.00), 第33-39段落 & JP 2000-23137 A, 第61, 66, 67段落 & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11, 25, 31
Y	JP 9-115241 A (ソニー株式会社) 2.5月.1997(02.05.97), 第21, 22, 28段落 & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (ソニー株式会社) 30.11月.1999(30.11.99), 第16, 18, 19, 57, 58段落 & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9.7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	1-32
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98, 1998, p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
P A	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-33